



WHITE PAPER: Achieving Information Assurance in a Green Computing Environment

What Security Professionals Should Know as Information Security Evolves to Information Assurance

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

Table of Contents

2	Introduction	8	Looking for Sensitive Data
2	Information Assurance	9	Organizational Challenges
3	Paper Reduction Efforts	10	Summary
5	E-cycling and Data at Rest	10	How Savvis Can Help
6	Power Management and Conservation	12	About the Author
7	Mobile Computing and Telecommuting	12	About Savvis

Achieving Information Assurance in a Green Computing Environment

Abstract

Computer Security professionals have long been striving to provide access controls to protect sensitive information residing on electronic data systems, it also needs to be recognized that some of the same data may be at risk when it is stored and handled outside the computing environment. The efforts to reduce solid waste and help to clean up the environment may put sensitive data at risk if the process changes resulting from “Green Computing” initiatives are not reviewed from an Information Assurance perspective.

Introduction

Security programs for organizations have always fallen under the critique that the data protection strategy is only as good as the weakest controls. Consider the analogy of a picket fence; any pickets that are missing or lower than the others provide opportunity for someone to slip through the fence or over it. Computer systems continue to be under scrutiny for the application of security controls; however, as the data on computer systems continues to be the target of cyber attacks each year, certain physical security strategies are often overlooked, and consideration must be applied where sensitive data exists outside the traditional computing environment. This is especially true as transitions occur from paper to digital storage, or in “Green Computing” initiatives that may include paper reduction, e-cycling, and power conservation.

Mobile computing and telecommuting introduce many challenges as sensitive data moves outside the traditional network perimeter, and provide opportunity for data theft and breach of sensitive information. Computer security practitioners must look beyond the security of sensitive data stored on traditional computer systems, and understand processes that handle sensitive data throughout the company or organization in order to apply ubiquitous information assurance. This white paper will examine some of the common risks of information breach that exist when Green Computing initiatives are not implemented with proper safeguards, based on the author’s experience in risk reduction and remediation efforts. This paper examines an Information Assurance approach to reducing the risk associated with sensitive data and explores the security convergence and integration of securing Information Systems along with the security of sensitive information handled in day-to-day operations and processes throughout the organization.

“Mobile computing and telecommuting introduce many challenges as sensitive data moves outside the traditional network perimeter, and provide opportunity for data theft and breach of sensitive information.”

Information Assurance

Information Assurance (IA) is the term used most commonly by federal governments for the protection of data on military systems, and is often used interchangeably with Information Security. The U.S. Government’s National Information Assurance Glossary¹ defines IA as:

“Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.”

Achieving Information Assurance in a Green Computing Environment

Businesses are beginning to see that their security posture frequently matches or exceeds military security for some of the most sensitive data, and recognize the value of IA's strategy of risk management and mitigation over the granularity of the application of security tools and controls that are principle in Information Security. It is not suggested that Information Security implementations are inadequate or unnecessary, but rather that an IA approach of managing risk helps to close the gap where security is not always applied, and to integrate Information Security with Incident Response, Disaster Recovery, and Business Continuity. The purpose of this paper is to address the risk management that must be applied to Green Computing, as well as sensitive data that is not on a computing system and therefore is often overlooked by computer security professionals.

For many companies and organizations, proprietary and sensitive information is their most important asset, and protecting that data from theft or damage is just as important as protecting any other physical asset. Organizational leaders understand the loss of sensitive customer records or proprietary information may result in the damage to an organization's reputation.² Security practitioners using ISO 27001/27002 as a guideline or standard for Information System Security programs in commercial enterprises or private organizations find the standards have much in common with government data security efforts such as the US Department of Defense focus on the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG), which are designed to be used in an IA program. IA assesses and applies basic security principles to the data no matter where it exists — in the computer, transported electronically or physically, or on paper — and how it is stored, recovered when lost, and destroyed when no longer needed.

Paper Reduction Efforts

The US Environmental Protection Agency (EPA) reports that paper and paperboard products (including office paperwork) constitute the largest portion of municipal solid waste.³ As organizations implement Green Computing Initiatives, security awareness must be communicated throughout the organization to make sure any new process that is developed to reduce paper is reviewed for security risk. What was once stored on paper will now reside on computer systems in disk arrays, and existing paper records may be scanned into computer systems to reduce paper storage and archives. As this process proceeds, what was once locked in file cabinets or vaults must now be encrypted in secure computing systems.

Case Study: The e-Mail That Exposed Sensitive Medical Information

For example, in an effort to save paper, a clerk in the workers compensation department of a large organization that has over 35,000 workers at one location begins using a document scanner to replace handicap parking applications with JPEG files. Each person who does not have a State Handicap Permit for parking, but would like to receive a temporary permit for use at work only, fills out a paper form application that contains personal information including the medical reason he or she needs a handicap parking permit, with a signature from a doctor. The applications are stored onsite in a locked cabinet, and a copy was previously sent to the head office 30 miles away. When it was transmitted it was placed in a



² Russell, D., & Gangemi, G.T. (1991). Computer Security Basics. Sebastopol, CA: O' Reilly & Associates, Inc. (p.20).

³ Targeted Initiatives. (2008, September 9). Retrieved Dec 1, 2008 from Environmental Protection Agency web site: <http://www.epa.gov/osw/partnerships/wastewise/initiatives.htm>

Achieving Information Assurance in a Green Computing Environment

double sealed envelope and carried only by a bonded courier. To save on paper, the clerk decided to scan the original form instead of making a photocopy, and to save on the cost of the courier (as well as the expensive envelopes), the clerk e-mails the JPEG file to a counterpart at the head office.

The failure here was the opportunity to evaluate risk in the modification of the process in order to reduce paperwork. When the clerk was asked why this change was not discussed with the IT department, since the process was being put on the computer, the clerk responded that it was their understanding that the e-mail system was secure, because the message was not going outside the organization. A quick review found that, as expected, the JPEG files were unencrypted in both the sender's sent folder and recipient's inbox. Additional copies were being stored in the clear on the hard drives of both users' desktop workstations, and many of the JPEG files had been forwarded to other users on the system for review and authorization of the permits. None of the users involved stopped to think that the electronic version of the previous process was now no longer secure, or understood that features of electronic data security such as encryption would need to be implemented. Many users and administrators also assume that e-mail that remains inside the internal network is secure. It is not common knowledge that many privileged — and sometimes unprivileged — users have access to e-mail, as well as to the back-ups of the saved data.

There is no reason that this electronic process cannot exist securely, but the JPEG files that contain sensitive information about the applicant's health condition must be protected while stored and transmitted electronically, just as the old process protected the physical paper document. Records management tools are available to monitor e-mail traffic and determine new user trends in order to help identify potential risk.

One solution is straightforward. The organization was able to use encryption tools, which in this case were already implemented in other departments, to store the JPEG files encrypted, and to only attach encrypted versions of the JPEG file to the e-mail as the scanned form was sent to the head office.

During the remediation of the risk, the clerk learned how to recognize Personally Identifiable Information (PII) as the security staff provided a list of PII data, and learned that when converting a paper or any existing process that handles sensitive data to the computer, a consultation with a Risk Manager or IT Security is in order. The organization also realized that security awareness related to the Green Computing Initiative would need to be communicated to all employees, and that the internal Green Computing promotional material had to be modified to include review of process changes with IT Security and Risk Management.

Case Study: The RFP Response That Never Dies

Another case where paper reduction was implemented without prior risk assessment occurred when a municipal government applied a Green Computing Initiative to the Request for Proposal (RFP) Process when selecting vendors for contracted services and capital improvement projects.

“This led to unencrypted copies of these files on hard drives, in e-mail folders and on system back-ups.”

Achieving Information Assurance in a Green Computing Environment

The previous established process was to issue an RFP, and collect the paper submission of all responses in a locked workroom. Each submitter was required to submit 10 copies of their proposal, and was promised that when the contract award was made, all who submitted would either receive all 10 copies back in return, or a certificate that the 10 copies were destroyed by shredding. The committee or jury that reviewed all responses and selected the contractor (or finalists to be submitted to the council for a vote), kept very tight controls on each proposal. Individual bidders were required to supply Social Security Numbers and other sensitive personal data on forms in the proposal. Each proposal also may contain competitive and proprietary information.

To implement a paper-reduction process, the Purchasing Officer had the staff begin providing the RFP on a website as an Adobe PDF file. In response, vendors were encouraged not to use hardcopy, but to submit their proposal in electronic format using Adobe PDF file or Microsoft Word. The vendors were told they could submit their response via e-mail or on CD-ROM using surface mail or courier.

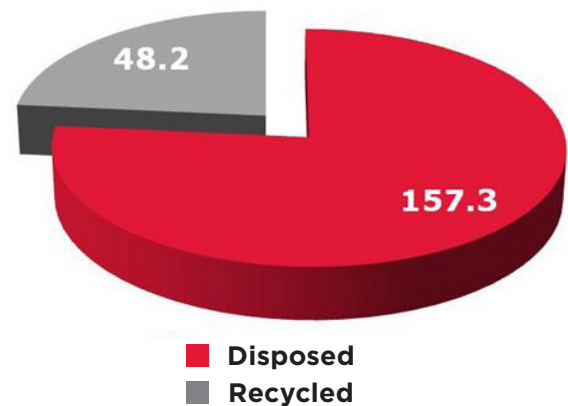
The IT staff was aware that Purchasing was putting the RFP on an externally facing website for the public to download a copy, but did not ask Purchasing what staff members were going to do with any electronic submissions they planned to receive. The Purchasing staff now began e-mailing the proposals among themselves, as well as among the committee or jury members. This led to unencrypted copies of these files on hard drives, in e-mail folders and on system back-ups.

Recommendations were made to discontinue the use of e-mail for transferring soft copies of RFP responses. Submitters would be allowed either to provide a CD-ROM with their soft copy response directly to the purchasing office via bonded courier, or to upload their submission to a secure website via an encrypted link. The purchasing office would have a choice of using a secure server to manage the soft copies of submissions or store them on a standalone system not connected to the network. In either case, the submissions would be encrypted when the data is at rest on the hard drive.

E-cycling and Data at Rest

In 1998, the National Safety Council Study estimated about 20 million computers become obsolete each year. Less than 10 years later in 2007, that number had more than doubled, according to the most recent EPA estimates resulting from a study on the management of used and end-of-life electronics. The EPA study showed that 65.7 million desktop computers and 2.1 million portable notebook computers accumulated in storage for surplus or disposal in 2007 alone.⁴ As the surplus grows, organizations are looking for ways to recycle or dispose of what is in storage. The EPA found that in 2007, more than 205,500,000 computer

U.S. Recycling vs. Disposal of Computing Products in Millions of Units during 2007



Source: EPA Report on Statistics on the Management of Used and End-of-Life Electronics.⁴

Achieving Information Assurance in a Green Computing Environment

products were recycled or disposed. Information security professionals must be involved in the definition of processes and procedures for disposal and recycling of computing equipment, to ensure that hard drives from notebook and desktop computers are either sufficiently overwritten⁵ to mitigate the recovery of sensitive data or destroyed. If an organization is not currently disposing or recycling computers, in time it is very likely this process will occur, and it must be supervised. When leasing equipment, consideration should be given in the lease to returning the notebook or desktop computer without the hard drive, especially if the owner is planning to refurbish the equipment anyway. This gives the user the opportunity to shred or destroy the drives themselves.

Case Study: The Surplus Surprise

A member of the Information Security team at one company accidentally discovered that the computer he purchased from the company surplus store for personal use contained proprietary data files that had not been overwritten (or even deleted) before the computer was recycled. This led to an emergency audit of all the computers in the surplus store and among 50 desktops that were available for sale to the public, four of those computers still had data that had not been removed.

The audit team traced each of the four systems back to the same source, and found that the company policy was not followed because the employee was unaware that the computers must be processed through the data services group first. Beginning immediately, a stop-gap measure was implemented in the surplus store to request the paperwork for the data services processing before the equipment is accepted. The importance of using the process for all end-of-life computing equipment was included in the next security awareness training program.

Power Management and Conservation

Several considerations are associated with the conservation of power as it relates to IA. First, the network equipment that resides in data closets needs cooling 24x7, and if the cooling in the building is being shut down on the weekends for power conservation, provision should be made to maintain cooling in those areas. Also, if cooling is shut down, desktops should be shut down as well, to prevent damage to electronic systems caused by overheating.

⁵ The DoD standard 5220.22 recommends overwriting non-sensitive data that should be difficult to recover three times using a three-pass overwriting algorithm (first pass - with zeroes, second pass - with ones and the last pass with random bytes), and seven times for sensitive, but unclassified data using a seven pass overwriting algorithm (first and second passes - with certain bytes and with its complement, then two passes with random character, and two passes with character and its complement and the last pass - with random character). Neither of these methods actually "sanitizes" the hard drive, which requires other physical degaussing and re-formatting of the drive. Most companies practice at least seven overwrites of proprietary data, and many have increased that requirement to 12 or more. NIST Special Publication 800-88, "Guidelines for Media Sanitization" provides specific recommendations on how to destroy hard drives and other computing devices that contain sensitive data.

Achieving Information Assurance in a Green Computing Environment

Once a power management plan is implemented that requires desktops or even selected servers to be shut down when not in use, concern shifts to how security updates will be picked up by systems that are shut off. Often, users have the ability to override a software update when it is triggered at boot time, so that it will not interfere with the urgency of their task. However, if power management is in use, and computers may be staying turned off for several days (or during the normal patch cycle), then the desktops must be configured to prohibit users from bypassing the update process when the patch is more than a week old (or if it is an urgent security update). Products are available to assist in making it an automatic process.

Certain systems and mission critical resources should be exempt from power management, especially security monitoring systems.

Mobile Computing and Telecommuting

In the 2008 Computer Security Institute (CSI) Computer Crime and Security Survey⁶, results showed that 42 percent of the respondents in the survey had experienced notebook computer theft in their company during the previous 12 months. The survey also reported that 17 percent experienced a theft or loss of customer data, half of which resided on mobile devices. The same group also reported that 45 percent of proprietary information that was stolen or lost was on mobile devices that disappeared.

Mobile computing devices such as notebook computers and smart phones or personal data assistants (PDAs) often contain proprietary or customer data stored by the user. Many users now carry USB memory sticks to transport data, which often is proprietary or sensitive in nature. Mobile computing devices are commonly stolen by thieves from home offices, a person's automobile or hotel room. Notebook computers and smart phones are also stolen from corporate and government offices as well.

If proper security controls are not used to secure mobile computing devices, data can also be stolen from these devices when they are connected to networks outside the Intranet. Most organizations include in their remote access policy for mobile computing users a prohibition on using public WiFi hotspots, unless a firewall is in use and Virtual Private Networking (VPN) software is used between the notebook computer and the organization's network. Several solutions may be implemented in an IA program to reduce the risk associated with mobile computing and telecommuting:

- **Telecommuting Security Policy:** All users who are using remote access should be connecting to the internal network through a VPN configuration. The preferred computing platform is one that is managed by the organization, but if the user is allowed to use their own computer, provisions must be made for anti-virus, firewall and security updates on the home computer. Employees should be reminded to store proprietary and sensitive information in a locked drawer, cabinet or safe in their homes when not in use. Make sure that they understand security policy for storage, transmission and destruction of sensitive data. Use of desktop virtualization can reduce risk of locally stored sensitive data.

Achieving Information Assurance in a Green Computing Environment

- **Encryption of Sensitive Data:** Notebook computer whole-disk encryption is growing in popularity, and many products are now available that are easy for users to operate. Several USB Flash Memory Devices with encryption are also available to make the transport of sensitive data on removable media easier and safer.
- **Physical Security Measures:** Notebook computer cables are recommended to secure notebook computers in use in the office or at home, reducing some risk of theft (this helps when the user momentarily leave the device). When the device is not to be used for the rest of the day, it should be placed in a locked drawer. Leaving these devices in a hotel room or automobile is normally prohibited by security policy. Anti-theft products are available that make a laptop traceable — as it places a silent call for help when it is connected to the Internet.
- **Remote Self-Destruct Mechanisms:** Keep an eye on new and improving technologies. Several notebook computers and smart phones will soon have the ability to allow an administrator to initiate a command to destroy data on the device the next time it connects with the network. USB memory sticks that self-destruct at the end of a given time period are also available.

Security Awareness Training on the use of Mobile Computing Devices and Telecommuting provides users with a better understanding of the risks, and how some simple precautions may reduce these risks and protect the sensitive data. Training should emphasize the special controls necessary for newly expanded boundaries of the network for mobile computing.

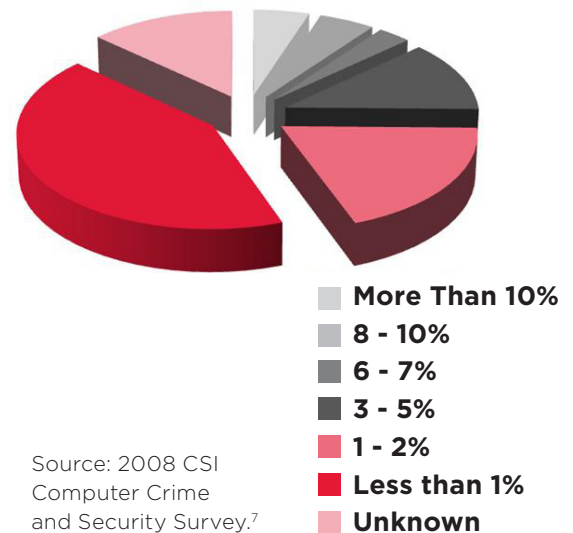
Looking for Sensitive Data

Once an IA program is established, information security team members need to continually think about where sensitive data might be found. During the next year, make an effort each month to physically survey each department in the organization. One-on-one interviews and location tours with staff members are the primary way to uncover sensitive data that is on standalone computers not catalogued, or in manual processes that may not even use the computing system.

Security professionals should make a special effort to not to make this review appear as an audit – rather it should be labeled as an information assessment. Use each visit as a way to spread security awareness, and promote the message that information security staff are available to help and enable the business, not to put in road blocks and make it difficult to conduct day-to-day tasks.

The 2008 CSI Survey also showed that most respondents of the survey spent less than 2 percent of the annual security budget on security awareness. For many organizations – this strategy of one-on-one visits to explain what data is sensitive as to how sensitive data should be handled, stored and destroyed – is a low-cost method to

2008 CSI Survey Results for Awareness Training as a Percentage of Security Budget



Source: 2008 CSI Computer Crime and Security Survey.⁷

Achieving Information Assurance in a Green Computing Environment

increase awareness⁷ among employees. Have a one-page chart that explains how to properly manage physical and electronic copies of sensitive data to leave with the employee, and encourage them to contact the information security team later if they have concerns or questions.

Case Study: Identity Theft Risk in Lost and Found Department

A tour of the Lost and Found department in a large public facility operated by a municipal agency uncovered the risk of articles that contain Personally Identifiable Information such as dozens of drivers licenses, passports, checkbooks, and credit cards.

Many of these items were sitting in the Lost and Found office for as long as 12 months. While the items stored in the facility were under the immediate supervision of the department staff, only jewelry was being locked in a safe. To reduce the temptation for an identity thief, a process was developed to reduce the amount of time the articles were stored before they were destroyed if the owner did not claim them, and a larger safe was secured to store these items while on the premises.

Organizational Challenges

Reaching out from the domain of the IT security department to begin asking about the IA implications in non-computing environments should be expected to be met with challenges. In many organizations, working with the physical or enterprise security entity early in the process will help to coordinate efforts. In some organizations, the two groups may form a joint task force to review the location of all sensitive information throughout the enterprise. Together, the individual security groups in the organization learn more about data that has been overlooked in the past, and can work together to mitigate risk.

When faced with the challenge of funding for this project, explain to management how the upfront investment in risk management and mitigation now will be much less than remediation efforts later to address the recovery from damage or loss of assets, and especially loss of reputation with the public or customers.

Using proper judgment to coordinate efforts with the support of senior management will result in greater cooperation. Request that a senior official, such as the CIO, write a letter to each department head explaining the importance of your survey and that this is a risk-reduction effort that will benefit every employee in the organization. Avoiding any appearance of an investigation or audit will result in more cooperation and openness. Invite participants to reveal their wish-list of items to be addressed and secured.

Be sure to plan meetings with key sources of potential sensitive information. For example, meet with the Director of Human Resources, then ask that person who on their staff will be most helpful in reviewing how data is currently handled, stored, and destroyed. Repeat this process in each business unit or department throughout the organization. Have a list of examples of sensitive data or PII to use as a checklist with each group.

Achieving Information Assurance in a Green Computing Environment

Summary

By using an IA program that includes a risk management step in any change to existing processes that handle sensitive information, organizations may implement Green Computing initiatives to benefit from the reduced cost while still remaining secure. Users must be educated as we look for ISO 14000 compliance⁸ and ways to reduce paper, recycle computer hardware, conserve power, and reduce fuel with telecommuting to understand the proper security controls that are necessary to protect sensitive data.

IT security professionals are already skilled in understanding threats and risk to sensitive data, and can evolve from computer security experts to Information Assurance specialists. Security convergence is achieved by locating sensitive data on electronic systems, as well as on paper or other media, and will enable the organization to implement an IA strategy that provides a balanced level of defense against data loss and theft.

How Savvis Can Help

Based on over 10 years of experience with clients seeking to outsource select portions of their IT infrastructure, Savvis has achieved a balance between people, process, and technology. No Information Systems Security Architecture solution is achieved by concentrating in just one area — an effective security solution requires a proper balance between each security discipline. Developing an Information Assurance program can place a demand on personnel resources, and Savvis has a team of experienced security consultants who may advise a client on policy development and maintenance, or provide services to establish new policy for an existing or planned environment.

Savvis is able to contribute to the success of any organization in meeting the goals presented in this paper. A brief examination of some of the tasks necessary to promote Information Assurance can yield concern over resources required to complete the effort to become compliant with security standards and build a security policy documentation set.

Outsourcing to Savvis

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

Savvis is an industry leader in Security Utility services

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

Achieving Information Assurance in a Green Computing Environment

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

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



Building an Information Assurance Program

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

The Savvis Information Assurance program strategy is to develop only policy or security standards that include requirements the organization is able to enforce. Savvis analyzes the current security posture and provides recommendations for adjustments to help organizations meet their specific security goals, such as the implementation of PCI DSS, DISA STIG, or ISO 27001 / 27002 security standards. Savvis consultants are experienced in adjusting security policy to support the organization's culture, mission and business focus. This results in the creation of a security policy that will be practiced by all users, staff, and management of the organization.

When necessary, Savvis is able to engage contributors with specializations in individual technical fields to produce a suite of security documents to support each customer's efforts for an effective security program. Examples of these areas include individuals with extensive experience drafting hardening standards for server and desktop platforms, network devices, and security devices; security patch management; network security standards; incident response plans; business continuity and disaster recovery plans; and proposing solutions for security measures such as centralized logging, intrusion detection, and file integrity, as well as other areas required to protect sensitive information as discussed in this paper.

Achieving Information Assurance in a Green Computing Environment

Savvis' Security Legacy

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

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

About the Author

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

About Savvis

Savvis, Inc. (NASDAQ:SVVS) is an outsourcing provider of managed computing and network infrastructure for IT applications. By outsourcing to Savvis, enterprises can focus on their core business while Savvis ensures the quality of their IT infrastructure. Leading IT organizations around the world have selected Savvis to help them improve their service levels, reduce capital expense and deal with the rising costs of bandwidth, energy, real estate, staff and expertise. As a pioneer in utility computing, Savvis understands and harnesses the latest advances in technology like virtualization, cloud computing and support process automation.

**For more information
about Savvis, visit
www.savvis.net or
call 1.800.SAVVIS.1
(1.800.728.8471).**

EMEA
Savvis UK Limited
Tel +44 (0)118 322 6000

ASIA PACIFIC
Savvis Singapore
Company Pte Ltd
Tel +65 6768 8000

JAPAN
Savvis Communications K.K.
Tel +81.3.5214.0151