The Information Leader

Winter 2007
Volume 12, No. 1

A Quarterly Journal on Information Trends by the World Leader in Information Resources Management Education

The Perfect Graduate

By Daniel J. Ryan and Julie J.C.H. Ryan

I. Introduction

There are currently seventy-five Centers of Academic Excellence in IA Education, including the Information Resources Management College of the National Defense University and the George Washington University. Each Center strives to turn out the perfect graduate, a knowledgeable, thoughtful individual who is fully capable of practicing the arcane profession of information assurance (IA). Some of these institutions base their programs on a foundation that is primarily computer science, others on an underpinning primarily of systems engineering, and still others on a management or business basis.

In each case, however, the multidisciplinary nature of the problem – protecting confidentiality, integrity and availability of information assets and the systems and networks that contain those assets – means that a perfect graduate needs to apply not only IA techniques and skills but also needs to be able to allocate resources, manage life cycles of technology solutions, supervise others performing unique tasks, and measure and communicate progress. In other words, the ideal graduate will need to be introduced to knowledge, skills and abilities that range far outside the IA foundation. This paper explores the range of subjects with which the perfect graduate needs more than a passing familiarity.

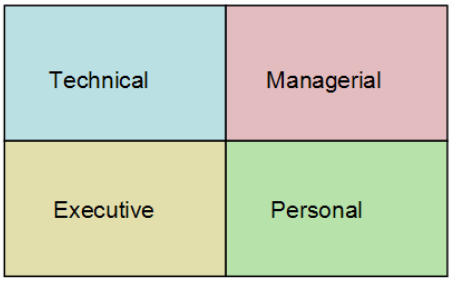

Figure 1: The Perfect Graduate's Skill Set

The perfect graduate of a program in IA needs a balanced mix of technical, managerial, executive and personal skills. This is not to suggest that a student who achieves a doctorate in a specific field, say mathematics, and who then specializes in the application of that field to certain problems in information assurance, say cryptographic systems, is not an IA professional. She is, just as surely as an M.D. who specializes in neurosurgery or a lawyer who specializes in antitrust litigation, are professionals in their own fields. But the perfect graduate will have a broad foundation and be able to bring to bear a variety of different skills and approaches to solving IA problems, and specialization must follow acquisition of that broad base.

II. Technical Skills

The perfect graduate must, of course, be capable of using tools, procedures and the specialized knowledge we offer in our programs to enhance the security of our information assets and systems. The problem addressed by IA is, at its core, mostly about the information, and less about the media and technologies used to create, store, process and communicate the information. Nevertheless, computer systems and networks are so closely tied to information processing in much of the world today that the perfect graduate needs to very comfortable with such systems and networks. It isn't necessary to be a computer scientist, but the knowledge of computers and networks that is required is certainly greater than would be required for practitioners of many other professions. A working knowledge

(Continued on page 2)

Contents

IRMC Information Resources Management College
The IRM College is a global learning community for government's most promising informaton leaders.
National Defense University

The Perfect Graduate

(cont.)

(Continued from page 1)

of computer and network architectures, circuit and packet switching, the ISO internetworking layers and protocols, routers, gateways, modems, directory services, storage and transmission of data, input and output devices, types of memory, firmware, system and application software, and so forth are essential to understanding attacks, defenses and models of trust.

An understanding of systems engineering is also desirable. IA is multidisciplinary, and systems of systems are common in information technology. In fact, some of the most critical vulnerabilities come from the interconnection of systems into larger systems. An understanding of how systems are designed, developed, implemented, integrated, tested, deployed, operated and maintained, and eventually decommissioned is therefore essential to a professional that must consider security at every stage of the system's life cycle.

Mathematical skills are also needed. Galileo Galilei said, "Mathematics is the alphabet with which God wrote the Universe." Math is required for computer science and systems engineering, of course. Also, one of the most valuable tools in IA – cryptography – is inherently mathematical in nature and requires an understanding of modular arithmetic, algebra, number theory and numerical analysis. Moreover, risk analysis and risk management requires an understanding of probability and statistics. A strong familiarity with the language and application of mathematics is crucial for the critical analysis, management, and engineering of IA solution sets.

Methods for improving or optimizing performance and for allocation of scarce resources make some skill in operations research (OR) an ideal subject for the perfect graduate. Understanding OR mathematical models, algorithms, and applied mathematics, including linear programming, stochastic programming, control theory, game theory, mathematical economics, and financial mathematics is also desirable. In certain IA specialties, other scientific knowledge may be valuable, such as knowledge of quantum physics, chemistry, or metallurgy.

III. Managerial Skills

The perfect IA graduate will be more than merely technically competent. The perfect graduate will also be prepared to manage the IA function. Whether the task is to create a new security product, deliver a security service, or secure an information infrastructure, a variety of managerial skills is needed in the practice of the IA profession.

Planning skills at the program or project level will be important. Through planning, our graduates assess the potential impacts that will flow from decisions they are making. Developing specific statements of requirements, anticipated accomplishments, measurable milestones, and appropriate metrics for measuring progress are critical skills. Understanding how to estimate the time, monetary, and personnel resources required to achieve planned goals is fundamental. The planning skills described here are narrow, specific, tactical skills. Strategic planning is an executive skill that will be addressed later in the paper.

Organizing is another critical skill. The perfect graduate will understand how to collect and configure resources to achieve security objectives in an efficient and effective manner. Task and project analysis skills inform correct definition and designation of roles within the security organization. Security employee job descriptions and personnel performance planning are crucial to the success of the organization. Managing the interfaces between security tasks and other organizational elements requires a deft touch and an ability to communicate with non-security employees. Knowing how and why to hire people with the right IA knowledge, skills and abilities, and how to keep them once on board, are management skills our graduates must master.

Managing to achieve cost, schedule and technical performance goals is essential. Channeling and orchestrating the activities of security professionals to achieve the security needed by the organization at an affordable price requires discipline and creativity. Furthermore, these skills must transcend the system life-cycle phases from development through replacement.

(Continued on page 3)

(Continued from page 2)

As noted above, a keen understanding of the use of metrics in controlling performance is crucial. The late, great management consultant Peter Drucker said, "If you can't measure it, you can't manage it." The perfect graduate will understand that simply counting things because we can count them does not measure real security. Counting policies written or security technologies implemented tells us little about the actual security we enjoy.

As Albert Einstein said, "Not everything that can be counted counts and not everything that counts can be counted." Security is especially difficult to measure since, after all, the best thing that can happen is nothing. But the perfect graduate knows that security is best measured by calculating expected loss as a function of time and the consequences of successful attacks on information assets and systems, and calculates returns on security investments by measuring reductions in expected losses. The perfect graduate will understand the difference between efficiency and effectiveness, and that efficiency does not necessarily imply effectiveness, and vice versa.

"...a perfect graduate needs to apply not only IA techniques and skills but also needs to be able to allocate resources, manage life cycles of technology solutions, supervise others performing unique tasks, and measure and communicate progress."

IV. Executive Skills

In addition to being taught good management skills and practices, the perfect graduate will have acquired a variety of executive-level skills. For example, strategic planning for the security function addresses three questions:

- What is our security status or posture today?
- What do we wish our security status or posture to be?
- What do we have to do to get from where we are today to where we want to be?

Answering the first of these questions requires a thorough and competent vulnerability assessment, including a review of existing policies, practices and procedures; mapping the information infrastructure; assessing threats; and evaluating strengths and weaknesses. Creating the vision for a more secure future and planning the path forward to that future are executive skills a perfect graduate will certainly understand. This strategic planning must clearly be done within the context of the enterprise's operational environment, which means that the perfect graduate must also be able to appreciate the operational necessities of other focus areas, such as production, and communicate effectively with the managers and specialists in those areas.

Executive management of the information security function is grounded in policy. At the organizational level, policies will control IA practices and procedures from access control to use of the Internet to acquisition of security technologies. Policies will determine who gets to make decisions about IA and who enforces those decisions. Policies will establish what needs to be protected, how much protection is needed, and how long protection must continue. Policies will dictate who can be hired, what information assets and systems they can use in order to perform the functions for which they were hired, and what they can and cannot do with those information assets. The perfect graduate will be comfortable with the use of policies and competent to analyze the impacts of policy decisions on the organization and on its ability to secure the information technology on which it relies.

Since policy can both be influenced by legal and regulatory oversight, and can also be considered within the context of differing jurisdictional standards, the perfect graduate must also be able to consult legal resources, and work with legal counsel, as to the appropriate language and implementation processes for IA policies. The perfect graduate must appre-

(Continued on page 7)

Practical VoIP Vulnerabilities

By Aaron Schulman and Dr. Robert Young
Information Assurance Laboratory

1 Introduction

Deploying a Voice Over IP network that is not secured can result in unauthorized release of sensitive information, inappropriate use of resources, and denial of service. In this paper we outline three prime vulnerabilities in Voice Over IP. Then we show how these vulnerabilities can be removed. Understanding this document requires an intermediate understanding of IP based networks, and a basic knowledge of telephone systems.

1.1 What is VoIP?

If you work in the IT sector there is a very good chance you have heard the acronym VoIP used around your office, and you may wonder, what is VoIP? VoIP or Voice Over IP is a technology that moves voice communication from a traditionally hybrid analog and digital infrastructure, the Public Switched Telephone Network (PSTN) to an all-digital network, carried over a Local Area Network (LAN) and/or the Internet. VoIP has existed since the mid-1990s but did not become popular because it was plagued by implementation issues. Now in 2006, we have reached the point where VoIP is fully executable and it is starting to hit the market with full force; boasting lower costs and more features, Gartner Research believes "the sale of new IP-PBX systems will surpass that for traditional PBXs," and eventually, "IP-telephony solutions will represent 90 percent of new system sales."

1.2 Who is using VoIP?

Many companies and governments are currently in the process of transitioning from PSTN to VoIP. The largest company making the transition is Boeing, putting together a VoIP implementation that will consist of 150,000 phones worldwide. In the US Federal Government the Department of Defense (DoD) began the move to VoIP in 2004. The DoD's Joint Interoperability Test Command (JITC) gave Cisco's VoIP PBX2 certification and subsequently organizations within the DoD began rolling out VoIP solutions. In 2005 the JITC also gave Cisco's VoIP PBX1 certification, which authorizes the use of Cisco's VoIP technology within mission critical environments.

2 Session Initialization Protocol

2.1 What are the components of most VoIP Networks?

VoIP networks are composed of two types of components, hardware and software. Software provides the means to signal handsets and other VoIP networks about incoming calls and also the ability to transfer the digitized voice signal. Several vendors, including Cisco and Avaya, produce VoIP software products. There is also a full-featured free Open Source solution called Asterisk. There are many standardized protocols used to signal VoIP handsets but most VoIP software is configured to use either SIP (Session Initiation Protocol) or H.323, although SIP has the most popularity. Cisco is a strong proponent of SIP; in one of their documents over-viewing VoIP they declared, "Many people believe that SIP will become the de-facto standard protocol for future voice networks."

2.2 What are the components of a SIP Network?

There are three main hardware components in a SIP network; the first and most important are VoIP handsets (see Figure 1). These resemble PSTN handsets but instead of attaching to a PSTN they attach to a LAN via an Ethernet Cable or Wireless Network (802.11a, 802.11b, 802.11g).

Source: Cisco Systems

Figure 1: Cisco IP Handset

SIP-based networks also need a way of knowing where a call signal should be delivered as it comes into or out of a network; this service is provided by the proxy server. A proxy server is set up to look up the appropriate IP address or VoIP network where a handset is lo-

(Continued on page 5)

(Continued from page 4)

cated. Proxy servers can be seen as the PBX of VoIP networks, routing calls to their appropriate destination. One advantage of a VoIP network is that the phones can be located anywhere in the world so long as they are connected to the Internet. You may wonder then, how does the proxy server know where the phone is currently located? This work is done by the registration server. The basic theory behind a registration server is as such: When a handset is connected to a network either inside the LAN or via the Internet, a repeating registration signal is sent from the handset to the predefined registration server. This signal informs the registration server of the handset's current IP address. This address is stored in the server's lookup database. When a proxy server receives a phone call, it queries the registration server for the current IP address of the destination handset and subsequently sends the signal. Finally the endpoint handset will receive the signal from the proxy. This signal contains the address of the handset that is placing the call. Following this the handset will establish a connection directly to the caller and a conversation can begin. To see the structure of a VoIP network using SIP see Figure 2 .

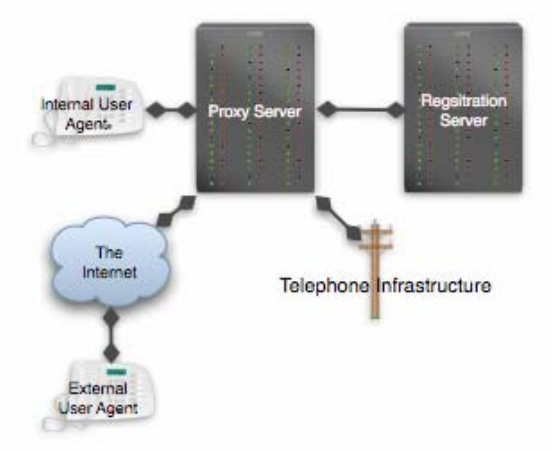

Figure 2: SIP Network Diagram

3 Vulnerabilities

3.1 SIP Registration Hijacking

Now that we have established a footing in VoIP networks implemented with SIP, we can examine the inherit vulnerabilities. In order to make this discussion clear I will use LH to indicate a legitimate handset and AH to indicate an attacker's handset. We have already seen that when a handset is connected to a network it will register with the registration server and continuously send registration information. The first vulnerability takes advantage of the fact that there is no permanent connection for sending signals. An attacker can send a registration signal to the registration server in between registrations made by the LH. If this signal contains the address of a handset that does not exist, the attacker will cause a Denial of Service. For example, if a call is placed to the LH after our malicious registration signal is sent, the proxy server will query the registration server for the IP address of the LH, but the address returned will point to a nonexistent device, so the signal will never reach the intended destination.

This attack can be further expounded by sending the malicious registration signal with the address of the AH instead of a nonexistent phone. If an incoming call is made to the LH the proxy server will send the call signal to the AH and the AH would ring instead of the LH. This would allow you to not only stop the LH from receiving calls, but also give the attacker access to calls that were intended for the LH. This attack is known as registration hijacking.

3.2 Wiretapping

Wiretapping a VoIP network can range from an extraordinarily easy task to one that is almost impossible depending on the VoIP network's configuration. One may think that most VoIP software will encrypt voice traffic and thus thwart wiretapping but in reality extra equipment is required to encrypt VoIP conversations at the transport layer. Specialized phones are needed to encrypt traffic at the network layer. This added expense forces many implementers to forgo encryption.

The network architecture that is most vulnerable to wiretapping is where VoIP devices are connected directly to an organization's LAN and hubs are used as the primary interconnection devices. In this network configuration any wired connection into the network will be able to passively listen to VoIP traffic using freely available sniffing software. In our lab we have tested a free open source program called VoIPong. This program runs as a daemon waiting for VoIP traffic to pass over the network. When traffic is seen it sniffs voice packets from both sides of the conversation, combines them into one data stream and saves the conversation as a .wav file tagged by the date and time. An attacker could install this piece of software on a laptop, obtain access to an organization's facility, and leave the laptop in a place where it is powered, has network access and is hidden. Then, every night the laptop will run a

(Continued on page 6)

VoIP (cont'd)

(Continued from page 5)

program to compress the audio received that day and upload the data onto a server run by the attacker. This same attack can also be performed by gaining access to a machine inside the organization and performing an exploit to execute the wiretapping software.

3.3 Configuration

As with any network service, security in a VoIP network depends heavily on configuration. Most of the configuration vulnerabilities in VoIP networks arise exist due to the tradeoff between security and convenience. Often organizations will implement a very simple password scheme for authentication of their VoIP phones. For example, they may use the same username and password for every phone on the network. In order to find out more about a large-scale VoIP configuration, we signed up for a popular consumer Internet-based VoIP solution. The provider sent us a VoIP gateway, which connects to a standard PSTN phone and encodes the analog data from the handset into VoIP traffic.

Using Wireshark, a free packet sniffer, we discovered that when the gateway powered on, the configuration was downloaded from the provider. This is convenient for the provider's administration staff because it allows them to modify the parameters of our phone's subscription, for example adding new lines can occur without the device being powered on. Closer inspection of the sniffed data revealed that the device's configuration information was downloaded from an open, non-encrypted web server that was hosted by the provider. The file name of the configuration file being sent was the same as the MAC address of our phone. Opening this file in a web browser revealed our phone number, SIP username and password used to authenticate with the proxy server, and our caller id name. The data appeared as such (the actual values have been modified):

LINE1NUMBER=2222222222

LINE1CALLERID=JOHN DOE

LINE1AUTHUSER=11111111

LINE1AUTHPSWD=11111111

Listed here is enough data to setup a VoIP handset that can place VoIP calls using John Doe's account. Also, if Mr. Doe's device is disconnected from the network an attacker can receive his incoming VoIP calls.

4 Securing VoIP

4.1 Authentication

Increasing authentication requirements for VoIP handsets will thwart attackers from unauthorized use of accounts. A password policy should be created that requires a unique password for each device. Also, passwords should not be derived from their handset's identifying information, including username, manufacturer and model.

4.2 Authorization

A VoIP network configured with authorization will only allow handsets to register or place calls if they are given exclusive permission. Configuring a network with authorization is time consuming because every new device brought onto the network will have to be manually authorized. Authorization's main benefit is protection against Registration Hijacking. If an Attacker's Handset is not authorized to register with the proxy server they will be unable to deny service or gain control of an account. Authorization also protects against configuration-based attack because the Attacker's handset will not be authorized to use the legitimate user's account even if they have gained the information needed to authenticate.

4.3 Physical Access

Many VoIP handsets are configured to use a default password for configuration changes. If an Attacker can touch the handset, they can use this password to gain access to the handset's configuration and thus will be able to gain knowledge of the proxy server's address and possibly the handset's authentication information. In order to perform the Registration Hijacking attack, the Attacker must have knowledge of the proxy server's address and this is an easy way to discover it. Implementers should change default configuration passwords on VoIP handsets to avoid this attack.

(Continued on page 7)

(Continued from page 6)

4.4 Encryption

The best way to prevent wiretapping in VoIP networks is to encrypt the traffic. Internal network traffic can be encrypted using network layer IPsec. This is achieved by using handsets with IPsec capability.

5 Conclusions

Armed with knowledge of the three major vulnerabilities in VoIP, is it our hope that managers will become more familiar with their VoIP security posture. However, the reader must understand that the defense measures presented in this paper will not prevent every attack on a VoIP network.

In conclusion, a Voice Over IP network that is secured with the methods shown in this paper is an inexpensive, and highly capable replacement for an analog telephone network. But always remember, phone calls made to a party outside of a local VoIP network will have to be handled by a network outside of the organization's control. Even if the conversation is encrypted within the local network, it will have to be unencrypted and sent in the clear to the outside.

6 Acknowledgments/References

We are appreciative of David Fraley, Shannon McCarthy, and Michelle Hugue for their beneficial comments. References are available on request.

Perfect Graduate (Cont.)

(Continued from page 3)

ciate the perspective and specialized language of such legal counsel and be able to communicate effectively with her.

Policy in the form of international, federal and State laws and regulations impact the organization's participation in national and global information infrastructures. National and international laws criminalize certain behaviors in cyberspace from hacking to abuse of authorized access to copyright violations. Other laws and regulations impact IA activities through regulation of ecommerce, privacy protection, taxation, competition, and a host of other rules and regulations that form the legal environment the perfect graduate must understand and navigate in the practice of our profession.

The perfect graduate will be able to function at the executive level because of a deep understanding of decision theory, both as a paradigm and as a set of tools for constructing and analyzing models of information assurance. The immense complexity of the problems we face in securing information infrastructures at the organizational and national levels require sophisticated tools and methodologies to explore problems that are often poorly defined, where rarely is there a "best" solution in a mathematical sense, where the "best" solutions are often not the cheapest, and where competing equity and political interests and imperatives compel contradictory approaches.

The choice of evaluation criteria, development of mathematical models, identification of alternative solutions, application of the evaluation criteria to the possible solutions, and sensitivity analyses all require a firm grounding in decision theory, and that's *before* our perfect graduate begins implementation of a decision. Fortunately, powerful techniques are available to inform these difficult decisions, and our perfect graduate will understand those techniques and be comfortable using them.

V. Personal Skills

Beyond the technical, managerial and executive skills that shape the perfect graduate, a variety of personal skills and characteristics is essential. Personal skills are needed to build relationships, solve human relations problems, and relate to others in ways that are consistent with and promote the goals of IA for the organization.

The perfect graduate will have excellent communication skills, written and oral, and will be able to communicate effectively

(Continued on page 8)

Perfect Graduate (Cont.)

(Continued from page 7)

and persuasively to others at all levels of the organization. The perfect graduate will be able to modulate the tone and technical content of both written and oral communications depending on the intended audience.

The perfect graduate will be a critical thinker, unwilling to naively accept proffered facts or statistics without knowing how they were collected and analyzed, yet not so cynical as to refuse to accept any data or statistics that could inform and guide the practice of her profession. The perfect graduate knows that good statistics are based on more than guesses or anecdotal evidence, that explicit, reasonable definitions were used in constructing the statistics, and that reasonable measurement criterion were employed. Making hard decisions about complex problems where the stakes are high, as is the case in IA, requires not only resolve but also a willingness to ask tough questions and require well-considered, persuasive answers.

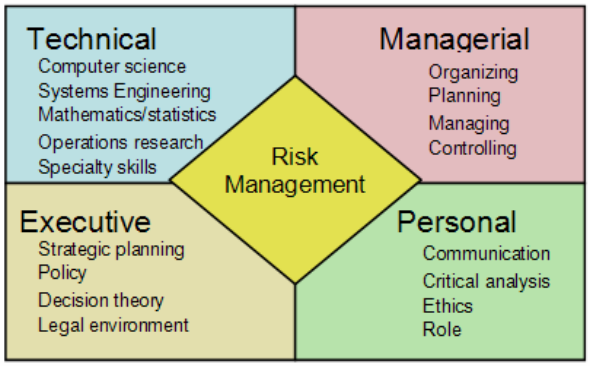

Figure 2: The Role of Risk Management

The perfect graduate will be characterized by a strong sense of personal and professional ethics, and a keen sense of the moral dimension inherent in decisions about information assurance. Our profession has no room for ethically challenged practitioners, and no need for moral compromises or expedient behavior.

The perfect graduate has a strong sense of the role of IA professionals. The perfect graduate understands that we are charged with managing risks that have more than local implications, that we are protecting valuable information assets and systems for our organizations, and that in so doing we collectively participate in the protection of our critical information infrastructure and thus of our nation's security and our way of life.

VI. Conclusions

As educators, the faculties of Centers of Academic Excellence in IA Education are responsible for creating future generations of IA professionals. Our graduates will bear great responsibility, for theirs is the task of securing our information infrastructure, the failure of which would have grave consequences for our economy and our national security. Our curricula, our lectures, our materials, and the projects we assign and research we direct must be designed to produce knowledgeable, thoughtful graduates who are technically capable of solving complex problems, but who are also much, much more. Our graduates must be taught to effectively and efficiently manage the IA function at the project, program, organization and enterprise levels.

They must be instructed in the use of executive skills for strategic planning, policy development and analysis, and decision theory. And the perfect graduate, having mastered all these skills and abilities, will also have learned to communicate effectively, to think critically, and to practice our profession based on strong and sound personal and professional ethics. The perfect graduate will understand how IA manages the risks to information assets and systems, and has been prepared by his tutors to assume responsibility as a professional for protecting our national and economic security by securing our critical information infrastructure.

Our graduates will bear great responsibility, for theirs is the task of securing our information infrastructure, the failure of which would have grave consequences for our economy and our national security.

E-Government….Revolution or Evolution?

By Col Michael Helsabeck, US Joint Forces Command and E-Gov Student

This article focuses on the progress of e-government; electronic government initiatives; and e-government implementation and leadership challenges faced by administrations over the past five years. Today we see the letter "e" attached to a growing list of words; eTrade, eCommerce, eLoan, eHarmony, eCulture, etc. etc. So the notion of e-government should not be that strange to most Information Leader readers. In its simplest form, the "e" can be thought of as shorthand for electronic.

E-Government involves the use of information technology to transform government business processes and operations, engage citizens, and provide government services. It is shorthand for a wide range of activities and goals that have grown out of a long history of government reform and reinvention efforts. E-government encompasses a wide range of activities and actors.

Todd Datz, writing in the March 1st 2003 issue of CIO Magazine, wrote, "E-government is designed to make it easier for citizens and businesses to access government information and services by encouraging interagency IT initiatives that, while improving customer service, also consolidate redundant systems, decrease paperwork, increase productivity and save money."

Background on Management Reform/E-Government

The role of IT in reform and reinvention was highlighted in the Paperwork Reduction Act of 1980 which mandated an Information Resources Management (IRM) approach to federal data. Vice President Gore's 1993 National Performance Review (NPR) took the idea further by seeking to make government more business-like and use technology to replace agency-centered processes with flexible results-centered solutions. The 1995 Paperwork Reduction Act established IRM strategic planning principles while the 1996 Clinger-Cohen Act ushered in a host of IT directives. The 1998 Government Paperwork Elimination Act opened the door for electronic documents/records and signatures to be accepted by the government, in effect giving them legal status. One of the President's Management Agenda (2001) government-wide initiatives was expanded electronic government. The President's Management Agenda (PMA) initiative to Expand E-Government delivered significant results to the taxpayer and federal employees alike. The culminating act was the passing of the E-Government Act of 2002 signed into law by President Bush on 17 December 2002. In a statement released following the signing of the act, Sen. Joe Lieberman (D-Conn.), author of the act, said "The idea behind this law is for the federal government to take full advantage of the Internet and other information technologies to improve its efficiency and to secure its electronic information". The Act also assists in expanding the use of the Internet and computer resources to deliver Government services, consistent with the reform principles outlined on July 10, 2002 by President Bush, for a citizen-centered, results-oriented, and market-based Government.

Sectors of E-Government

In 2002 the E-Government Strategy was published, identifying a set of 34 e-government initiatives, and other related efforts. These initiatives are divided among four key portfolios: Government to Citizen (G2C), Government to Business (G2B), Government to Government (G2G), and Internal Efficiency and Effectiveness (IEE). In Jeffrey Seifert's "A Primer on E-Government: Sectors, Stages, Opportunities, and Challenges of Online Governance", he elaborates on three e-government sectors.

The Government-to-Citizen (G2C) sector facilitates citizen interaction with the government, which is seen by some to be the main focus of e-government. One prominent G2C example is Firstgov.gov, an online portal for 186+ million pages of government information, services and online transactions.

The Government-to-Business (G2B) sector seeks to reduce the cost of conducting business with the government for both businesses and the government. One G2B example is Buyers.gov, a business and auction exchange administered by the GSA Federal Technology Service.

As a G2G example, a homeland security initiative is a secure portal to improve the disaster management process by simplifying and unifying interaction between Federal, state and local public safety personnel (disasterhelp.gov).

The E-Government Strategy (April 2003) describes the fourth sector, Internal Efficiency and Effectiveness (IEE) dubbed Government-to-Employee (G2E) by Seifert and seen as a

(Continued on page 10)

E-Government….Revolution or Evolution? (cont.)

(Continued from page 9)

subset of G2G. One IEE example is GoLearn.gov which provides enhanced access to high quality training and competency development for federal employees.

Evolution Stages of E-Government

In addition to identifying e-government initiatives according to their sector, Seifert also describes four evolution stages of e-government development: presence, interaction, transaction and transformation. Accenture describes three maturity levels; publish, interact and transact. Presence and publish are simply making available information via the Internet. A typical example of presence is a basic Web site that lists cursory information about an agency, such as hours of operation, mailing address, and/or phone numbers, but has no interactive capabilities.

Interaction allows the user and agency to interact with each other short of completing an end-to-end transaction. Interactive web-based initiatives include instructions for obtaining services, downloadable forms to be printed and mailed back to an agency, and e-mail contacts to respond to simple questions. Transaction capable systems permit the completion of tasks done by non-electronic means previously. Examples of these initiatives include self-service tasks such as license renewals and paying taxes and fees.

The highest order of evolution for e-government initiatives is transformation. Initiatives at this level utilize the full capabilities of the technology to transform how government functions are conceived, organized, and executed. Transformational systems redefine how government functions are defined and delivered by removing organizational boundaries and providing customer-centric solutions. However, for a variety of technical, economic, and political reasons, it will take time for these initiatives to evolve into their full potential.

Reform Models of E-Government

Government reform driven by e-government in its three/four sectors and along the three to four stages of development has linkage to the four reform models presented by B. Guy Peters in his **The Future of Governing** book. The four models are the market government, participative government, flexible government and deregulated government. Many of the reform efforts spurred on by acts, commissions, reviews and agendas promote ideas from Peters' four government reform models. The President's Management Agenda, the E-Government Act of 2002, Clinger-Cohen Act of 1996 and Government Paperwork Reduction Act of 1998 promote market-based mechanisms to replace the traditional bureaucracy. The President's Management Agenda clearly lays out market model motivations in its vision for government reform; "Citizen-centered" (customer, consumer), "results-oriented" (efficient) and "market-based". A good example of market-based reform accomplished via an e-government initiative is IRS free filing (irs.gov). IRS free filing saves citizens and the government both time and money. The National Performance Review and President's Management Agenda brought about reform aspects of the participative model by promoting greater government transparency, citizen awareness and involvement. E-Rulemaking (regulations.gov) is an example of an e-government initiative allowing citizens to easily access and participates in the rule making process. Changes spawned by the implementation of e-government have caused organizations to be flexible as changes inevitably occurred. Tenants of the flexible model were not the objective of e-government as can more easily be seen in the market and participatory models. Cross boundary e-government initiatives force the greatest flexibility as agency boundaries become less important and functions/services take center stage.

As more and more transactions are accomplished via the internet or other technology, surge capacity can more easily be accommodated through IT vice employees. IT provided flexibility allows organizations to be more flexible in quickly expanding or decreasing capacity as needed. The National Performance Review and Paperwork Reduction Act reflect some of the ideas of the deregulated model. The National Performance Review saw the problem in government as the rules and regulations, not the people. Therefore, improvement could be realized by reducing the rules and regulations. E-government does not have as a major focus area the deregulation of government. The linkage between e-

(Continued on page 11)

(Continued from page 10)
government and the deregulated model of government reform is the weakest of Peters' four reform models.

E-Government Challenges

E-government is not without significant challenges, especially as e-government maturity moves from presence to transformation. In 2003 a group of more than 100 e-government project managers discussed challenges that the 2003 E-Government Strategy should address. Interestingly, none of the challenges involved technology, but rather behavior and policy. Leadership support, parochialism, funding and communication were cited in the April 2003 E-Government Strategy as challenges.

Leadership is needed to strengthen relationships between lead agencies, partner agencies, CIOs and the President's Management Council to improve how leaders work together to implement projects. Parochialism needs to be combated to address policies and budget practices that reinforce agency-centric thinking. Funding for more resources (dollars and staff) is required, along with a more transparent and effective budgeting process. Improved communication to help understand the relationships among e-government initiatives and key players is also required. Agency unique solutions need to be physically migrated to cross-agency solutions typically accomplished via portals like recreation.gov and managed by one or two service providers. Leaders are also challenged to recruit and retain the best and smartest people.

Accenture's 2004 study on e-government trends identified integration as a changing challenge. The study found "interest in horizontal integration has been apparent for some time; what is new are decided efforts to integrate vertically—across national, state/regional and local levels of government. Governments that attempt this level of integration face greater technical complexity as well as new challenges in organizing the governance and funding of these new initiatives."

In Jeffrey Seifert's "A Primer on E-Government…" he lists four potential e-government challenges: "Computer Security, Privacy, Disparities in Computer Access and Government Information Technology Management and Funding." Rosabeth Moss Kanter in her book **eVolve** addresses the challenge of change required to embrace e-culture, lead within it and build commitment. Kanter speaks of "deep systematic change, not cosmetic change, and a deeper emphasis on human skills that build meaningful community out of mere connections." Sound easy? Sound easy within the government? Kanter presents a case study on the significant difficulties Barnes & Noble had trying to compete with Amazon.com via the internet.

Progress in E-Government

Finding examples and information on unsuccessful e-government initiatives is much harder than efforts headlined as examples of e-government's promises being realized. When a project's warts are presented it is usually to show how far the effort has come and how successful it is now. No one likes to trumpet their "un-successes", especially in the government. Additionally, defining un-success is difficult and usually just a point in time on the way to some measure of success. G. David Garson in his "The Promise of Digital Government" presents a couple of struggling/unsuccessful efforts. Garson cites a 2002 National Institute of Governmental Purchasing survey showing virtually no increase in the percent of government purchasing agencies using e-procurement between 2001 and 2002, and South Carolina abandoned its e-procurement system. Garson also cites a Santa Monica e-democracy (PEN) example that fell into disuse after an initial tsunami of publicity and flurry of use. "Elected officials came to see PEN as a vehicle for hecklers and political junkies not representative of the community and not helpful as a forum for their exposure for purposes of re-election."

The government's 2005 expanding e-government results report, "Expanding E-Government: Improved Service Delivery for the American People Using Information Technology," highlights accomplishments and sets forth goals. Progress can be measured by reviewing previous reports completed in 2003 and 2004. The 2005 report available at http://www.whitehouse.gov/omb/budintegration/expanding_egov_2005.pdf, highlights accomplishments across the four e-government sectors: G2G, G2B, G2C and IEE. One specific effort highlighted is GoLearn.gov, providing e-training to federal employees. The site has more than 650,000 registered users and more than 1,300,000 courses have been completed. As of Dec 05, there were 6 agencies who had achieved "green" status on the President's Management Agenda E-Gov

(Continued on page 12)

E-Government….Revolution or Evolution? (cont.)

(Continued from page 11)

scorecard element. The 2003 E-Government Strategy highlighted GovBenefits.gov for information and services of over 400 government programs representing more than $2 trillion in annual benefits. The site received at the time over 500,000 visitors per month and was listed as one of USA Today's "Hot Sites". For a list of the Center for Digital Government's 2004 Best of the Web and Digital Government Achievement Award winners follow the following link: http://www.centerdigitalgov.com/bestof/?loc=29. In testimony before the Committee on Government Reform, Mark Forman spoke to the government's focus on 24 cross agency e-government initiatives grouped into G2G, G2B, G2G and IEE to consolidate redundant initiatives around citizen needs. Additionally six lines of business (LOB) have also been identified for even greater opportunities to streamline, integrate and consolidate IT investments spread across multiple agencies.

The Future of E-Government

The government's 2005 expanding e-government results report list five goals/keys to continued success for fiscal year 2006. The first goal is for agencies to continue using Enterprise Architectures to eliminate redundant business functions. The second goal is for 90% of agencies to have acceptable business cases for their systems. The third goal is for 90% of IT systems to be properly secured and IG verification of security remediation processes. The fourth goal is for 50% of agencies to close IT skill and competency gaps. The last goal is for 50% of agencies to manage their IT Portfolio using Earned Value Management and average within 10% of cost, schedule and performance objectives. Future e-government work can also be expected to continue moving forward along the lines of the LOBs and 24 cross-agency projects.

The 2004 Digital States Survey (www.centerdigitalgov.com) concluded much of the same roadmap for the federal government's future e-government efforts: "the future of digital government necessarily meant the continued build-out of citizen- and business-facing service delivery channels on the use of shared infrastructures and adherence to a common architecture that would tie formerly discrete government entities together."

Conclusion

In order to continue pushing ahead toward the goals of e-government, continued IT and services consolidation within lines of business and the creation of cross agency lines of business will be critical. The budget process along with Office of Management and Budget requirements should drive more effective and less redundant IT and e-government spending. To maximize the likelihood of success, future e-government initiatives should set clear and measurable objectives for constituency value, operational efficiency and political return. (Gartner research 2002) Initiatives should also tackle areas with low transaction complexity and high transaction volumes. (Gartner research 2002) Kanter also recommends small projects; one loaded for success and not requiring much change and one that demonstrates benefits. Organizations and individuals need to expect and be prepared to change. Building partnerships for collaboration across agencies within lines of business will also be important. Accenture's 2004 e-government study found that e-government advances were diminishing and slowing down. The Accenture study concluded effective e-government strategies must address improved delivery, rising stakeholder expectations of government services and improved cost-effectiveness in providing services.

The question remains, is e-government revolutionary or evolutionary? The maturity levels and development stages described by Accenture and Seifert respectively make the case for e-government being evolutionary. There was no popular uprising by citizens demanding e-government. E-government progress has also been deliberate and measured over the past five or six years. It is my assertion that e-government is evolutionary, as it is the continuation of governmental reform/reinvention by different means and powered by technology.

INFORMATION RESOURCES MANAGEMENT COLLEGE

The World Leader in Information Resources Management Education

300 5th Avenue Marshall Hall (Building 62)

Fort Lesley J. McNair, DC 20319
(202) 685-2096

http://www.ndu.edu/irmc/

GET ISSUES ONLINE: http://www.ndu.edu/irmc/out_infott.htm

Director: Dr. Robert Childs

Dean of Faculty & Academic Programs: Dr. Elizabeth McDaniel

Editor-in-Chief: Dr. Les Pang

Associate Editor: Dr. James Kasprzak