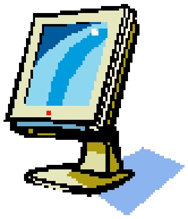
INFORMATION RESOURCES
MANAGEMENT COLLEGE

Fall 2002
Volume 7, No. 4



Info Tech Talk

A Newsletter on Enabling Information Technologies by the IRMC Information Operations and Technology Department

CobiT: Not Just Another Acronym

By Les Pang

What is CobiT? Is it a new car from Detroit? An element used for making blue glass and ceramics? Or a data bit that has lost its heat? Not really!

CobiT is an acronym for **C**ontrol **Ob**jectives for **I**nformation and related **T**echnology. It is a widely accepted standard for ensuring sound information technology (IT) security and control practices that provides a reference framework for management, users, and information systems audit, control and security practitioners. Taking a process focus and ownership perspective, it divides IT into 34 processes belonging to four domains (planning and organizing, acquiring and implementing, delivery and support, and monitoring) and provides a set of control objectives for each process.

The following are some of the IT processes addressed in the standard along with its reference number:

PO1	*define a strategic IT plan*
PO3	*determine the technological direction*
PO5	*manage the IT investment*
PO9	*assess risks*
PO10	*manage projects*
AI1	*identify solutions*
AI2	*acquire and maintain applications software*
AI5	*install and accredit systems*
AI6	*manage changes*
DS1	*define service levels*
DS4	*ensure continuous service*
DS5	*ensure system security*
DS10	*manage problems and incidents*
DS11	*manage data*
M1	*monitor the processes*

A control objective is a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity. One example of a detailed control objective is as follows:

"Senior management is responsible for developing and implementing long- and short-range plans that fulfill the organization's mission and goals. In this respect, senior management should ensure that IT issues as well as opportunities are adequately assessed and reflected in the organization's long- and short-range plans. IT long- and short-range plans should be developed to help ensure that the use of IT is aligned with the mission and business strategies of the organization."

CobiT applies to enterprise-wide information systems, including personal computers, mini-computers, mainframes and distributed environments.

The CobiT control framework consists of the following:

- **Management Guidelines** - provide guidance in assessing the status of the organization, identifying critical activities leading to success and measuring performance in reaching enterprise goals. These address maturity models, critical success factors, key goal indicators and key performance indicators for all of CobiT's 34 IT processes. These guidelines provide management with tools that allow self-assessment and choices to be made for control implementation and improvement over information and related technology.

(Continued on page 11)

Inside this issue:

"CobiT is...a widely accepted standard for ensuring sound information technology (IT) security and control practices that provides a reference framework for management, users, and information systems audit, control and security practitioners."

A Content Management System (CMS) on a Shoestring

By Jay Alden

The *NDU Knowledge Net for CIO's* is a website (www.nduknowledge.net) operated by the IRM College for CIO's throughout the federal government and their staff. It's run by a handful of faculty members who post information about and links to articles, websites, events, and documents that ought to be of interest to people working in CIO offices. One interesting aspect of Knowledge Net is that these faculty members – who we call *content managers* – can post, edit, and remove information on the website at anytime and from any location. And, their actions take effect on the website instantly; there are no middlemen in the process. You see, Knowledge Net has a *Content Management System* (CMS). We didn't buy one, we built it – or more precisely, two graduate students working at the College built it for us. Not bad huh? Let me tell you a little bit about our CMS.

But first, here are a couple of definitions of content management systems that I like:

"A Content Management System allows content to be stored, retrieved, edited, updated, controlled, then output in a variety of ways such that the incremental cost of each update cycle and output production shrinks dramatically over time." (http://www.press.umich.edu/jep/03-04/kartchner.html)

"A CMS is a tool that enables a variety of (centralised) technical and (de-centralised) non technical staff to create, edit, manage and finally publish a variety of content (such as text, graphics, video etc), whilst being constrained by a centralised set of rules, process and workflows that ensure a coherent, validated website appearance." (http://www.contentmanager.eu.com/history.htm)

Our vision: Knowledge Net is the first resource a federal CIO or staff member accesses when faced with a work-related challenge.

The no-frills CMS (like the one used with Knowledge Net) provides:

- An *Interface*: a simple-to-use web-enabled form that elicits the data elements for publishing.
- A *Data Repository*: the database that stores the data elements
- An *Output Utility*: the system component that formats the data for web publishing via a web server.

High-end content management systems also include:

- A *Workflow Scheme*: a system for scheduling work tasks for authors, editors, and managers, keeps track of data elements (e.g., entry time, output time, modification history) possibly providing a means for collaboration among team members, and certainly arranging for appropriate levels of approval necessary for web publishing of content.

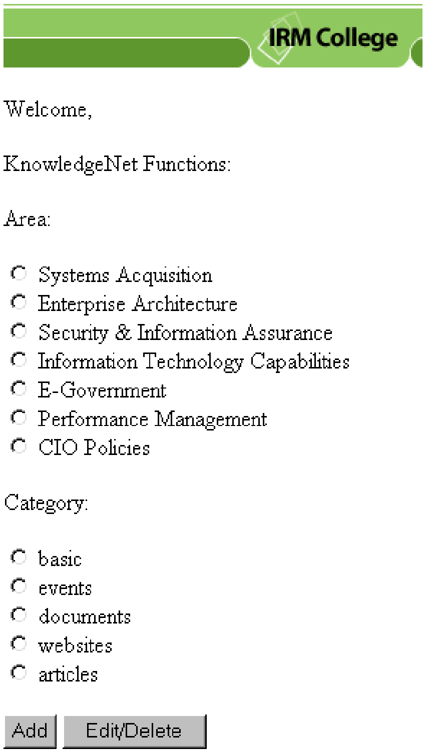
The high-end systems also include more bells and whistles in the other three CMS components than with the no-frills system. For example, the *Output Utility* in a high-end system can typically personalize the display based on the preferences and activities of individual users. For more information on content management systems in general go to http://www.cmswatch.com/ and http://guide.darwinmag.com/technology/web/content/index.html

The Knowledge Net CMS is of course a no-frills system. When the content manager has new information to load - such

(Continued on page 3)

(Continued from page 2)

as a reference to a recent article published in CIO Magazine - he or she logs in to a private Knowledge Net website with an ID and password. The electronic form shown to the right is displayed asking which of the six content areas covered by Knowledge Net (e.g., *Systems Acquisition*, *Enterprise Architecture*, …) and which kind of web page (e.g., *article, event*,…) is involved with the new information, and whether the content manager wishes to "Add" or "Edit/Delete" a data element in the database. After submitting his or her selection, another form is generated. If a data element is to be added, the new form (shown below) elicits entries for the particular kind of information required for the selected type of web page. For example, if a reference to that recent article in CIO Magazine is to be added, the form asks for the *title, URL, publication name, date of publication, author*, and a brief *summary* of the article. If the new reference was to a website, the "Websites" form would only request the *name* of the website, its *URL*, and a brief *description* of the website. With the information entered, the content manager clicks the Submit button and the new data element is entered directly into the Knowledge Net database.



Welcome,

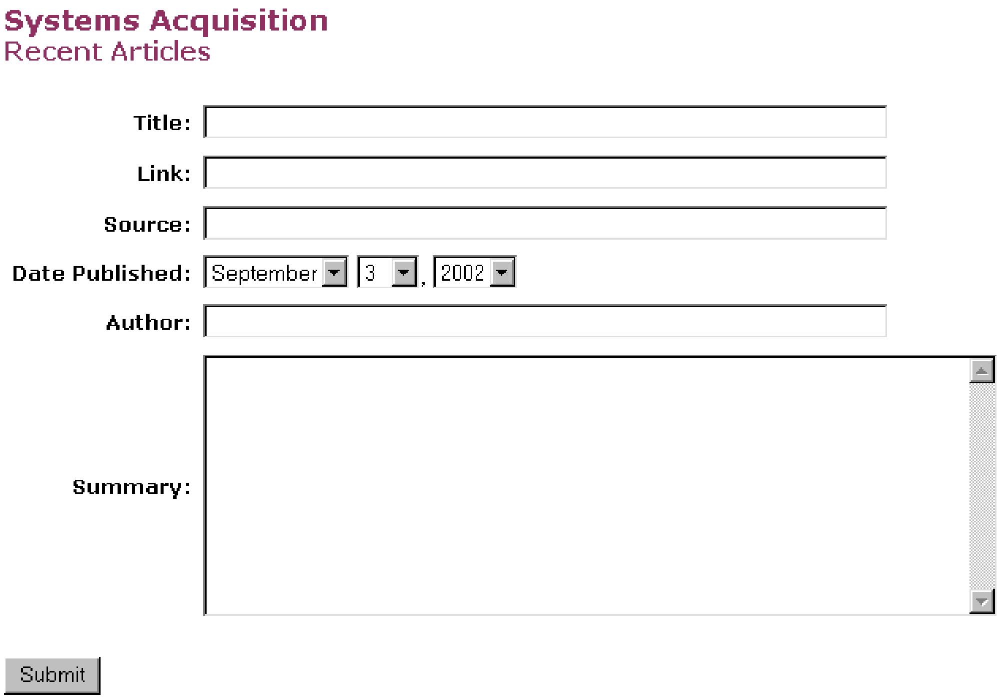
KnowledgeNet Functions:

Area:

○ Systems Acquisition
○ Enterprise Architecture
○ Security & Information Assurance
○ Information Technology Capabilities
○ E-Government
○ Performance Management
○ CIO Policies

Category:

○ basic
○ events
○ documents
○ websites
○ articles



Systems Acquisition
Recent Articles

Title:

Link:

Source:

Date Published: September 3, 2002

Author:

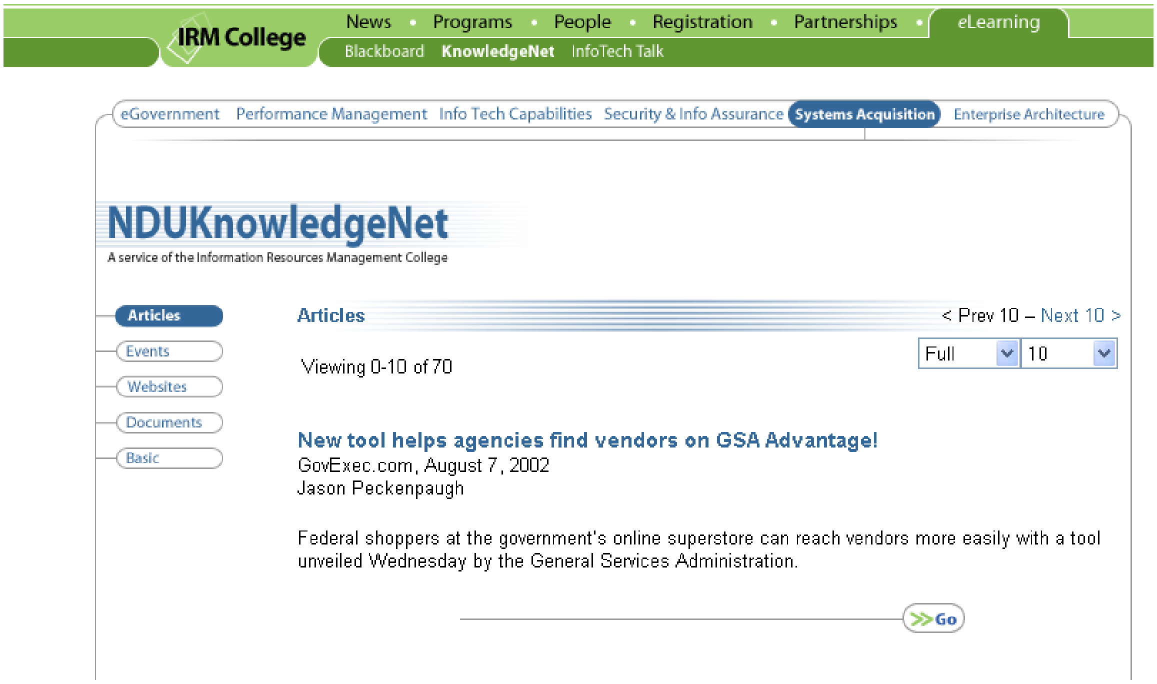
Summary:

(Continued on page 4)

A Content Management System (CMS)

(Continued from page 3)

The next time the updated web page is requested by someone over the Internet, the Knowledge Net *Output Utility* constructs the page on-the-fly (as shown below) based on the information currently in the database. So, even if a user requests a page one second after the content manager clicked on the Submit button to add a new item to that page, they would see the updated page. To someone who used to have to wait anywhere from three days to three weeks to see a new item uploaded by the "webmaster," the new CMS-based system seems magical.



Viewing 0-10 of 70

New tool helps agencies find vendors on GSA Advantage!
GovExec.com, August 7, 2002
Jason Peckenpaugh

Federal shoppers at the government's online superstore can reach vendors more easily with a tool unveiled Wednesday by the General Services Administration.

If a content manager wished to edit an item already posted to Knowledge Net (e.g., say they wanted to correct a misspelling or remove what is now a broken link), he or she would start off the same way as adding an item, but choose "Edit/Delete" instead of "Add." This selection would open a form showing every single item now in the database for the selected kind of web page in the chosen content area (e.g., all *Events* in the *Information Assurance* content area). They would locate the item to be edited or removed, and click on the button "Edit" or "Remove" accordingly. If they chose to remove the item, the system gives them one last chance to change their mind before eliminating all traces of the item from the database – and thereby vanishing from the display to users. If they opted to edit the item, an editable form opens where the content manager can change any of the fields. Upon submission, the revised item takes its place in the database for display at the next user request. It really is magical.

For the technical types among you, the database is created and managed with MySQL and the dynamic interaction is accomplished by the PHP scripting language. We chose these products because they're free, powerful, and are compatible with virtually all hardware and operating systems. Besides, these are the products that our graduate students knew.

The CMS has been a blessing for Knowledge Net. From my own experience, when I come across an appropriate item, I have it posted to the Web in less than a minute. This really helps us keep the content on Knowledge Net fresh. Visitors ought to check into Knowledge Net several times a day since it is now updated all the time. Some time in the future, we hope to extend access to the CMS by website visitors so that they can suggest items for Knowledge Net. We envision that the CMS will format visitor supplied items, submit them to the appropriate content manager who can reject them outright, modify them, or have them posted directly as is. Won't that be something?

With the CMS in place, we're almost finished with the first phase of Knowledge Net. We only need the search engine installed to complete the *publishing* function (due later this year). The second phase – which introduces a *discussion* capability so people in the field can initiate or participate in online discussions with faculty and other practitioners on issues with which they're concerned – is also due later this year. The final phase, in which we can begin *webcasting* presentations by guest speakers at College, should come early next year.

Going Wireless!

By Clifton Poole

The proliferation of wireless local area networks in the enterprise and home domains has increased dramatically within the past several years as the 802.11b protocol has emerged as the standard of choice for wireless communication. Just take a look at the networking section of your local electronics store and you will find a host of wireless networking products to complete your home or enterprise wireless network. I purchased my first of many wireless devices for my home network about 18 months ago and the product selection for the home user has quadrupled since that time.

Many corporations are now using wireless LANs as their preferred access methods within their facilities because of the solutions' ease of installation, reduced maintenance with moves and changes, and flexibility of deployment. Changing a network using wireless technology require fewer modifications to the physical environment. By using wireless devices to build a network, forklift upgrade - an upgrade to a computer network or other electronic system that requires a massive hardware investment-are greatly reduced. Wireless LANs also allow a user with a laptop the freedom to roam about his enterprise and still maintain access to the Internet and the rest of the network. The wireless solution is more elegant than running Ethernet when the computers are far apart from each other and users are still required to have access.

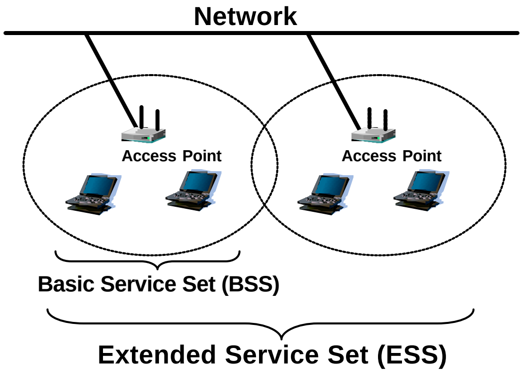


Figure 1: Wireless Infrastructure Mode

There are two types of wireless LAN connections available today -- private and semi-private. Private WLANs are by far the most prevalent among enterprises, allowing companies to inexpensively deploy technology that will permit employees to gain full wireless access to the corporate network. On the other hand, semi-private WLANs are private WLANs that also permit limited use for trusted non-private users such as a contractor working within an enterprise. In the public space, hotels, airports, shopping malls, convention centers, and even coffee shops are installing hot spots for use by their customers while they visit their properties. These Wi-Fi hot spots offer faster access to data for the on-the-go technical professional who needs high-speed access while away from the traditional office. The hotspots are not cellular towers, but 802.11b access points connected to the internet by a DSL, cable modem or an ISP.

The sheer volume of products and terms makes it difficult to understand what wireless is and how it will change your view of networking. Let me introduce you to a few wireless terms, explain how wireless networks operation, discuss wireless security and unusual wireless practices.

Definitions

802.11b is an extension to 802.11 that applies to wireless LANs and provides 11 megabits per second transmission in the 2.4 gigahertz band. 802.11b standard allows wireless functionality comparable to Ethernet. 802.11 is a family of specifications developed by the Institute of Electrical and Electronics Engineers (IEEE) for wireless LAN technology.

Access point is a hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN. Access points are important for providing heightened wireless security and for extending the physical range of service for a wireless user.

Wi-Fi is short for wireless fidelity and is another name for IEEE 802.11b. It is a trade term promulgated by the Wireless Ethernet Compatibility Alliance "Wi-Fi" is used in place of 802.11b in the same way that Ethernet is used in place of IEEE 802.3.

WLAN is a type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes. You will find WLAN networks configured for private use within business and home settings or as a public WLANs or Wi-Fi networks.

How does Wireless Networking Work?

The 802.11b standard defines two modes: infrastructure mode and ad hoc mode. In infrastructure mode, the wireless network consists of at least one access point connected to the wired network infrastructure and a set of wireless end stations. This configuration is called a Basic Service Set (BSS). An Extended Service Set (ESS) is a set of two or more BSSs forming a single subnetwork. Since most corporate WLANs

(Continued on page 6)

Going Wireless! (cont.)

(Continued from page 5)

require access to the wired LAN for services (file servers, printers, Internet links) they will operate in infrastructure mode. Here at the IRM College we have ESS which consist of over 15 access points and nume rous wireless clients.

Ad hoc mode (also called peer-to-peer mode or an Independent Basic Service Set, or IBSS) is simply a set of 802.11 wireless stations that communicate directly with one another without using an access point or any connection to a wired network. This mode is useful for quickly and easily setting up a wireless network anywhere that a wireless infrastructure does not exist or is not required for services, such as a classroom, meeting area, or airport, or where access to the wired network is barred (such as for consultants at a client site).

To take advantage of the 802.11b in either mode you have to have a wireless NIC installed in your device. The NIC is installed in an available PCMCIA slot and configured for use within the WLAN.

Security Methods

As WLANs become widespread, the need to business for a more robust security solution is required. Recent demonstrations of the vulnerability of Wired Equivalent Privacy (WEP) encryption make it clear that WEP protection alone is inadequate. A robust and scalable security solution is available by using Virtual Private Network (VPN) technologies or another robust authentication scheme. To safeguard data on WLANs, the 802.11 standard specifies three basic methods of securing access to wireless Access Points (APs):

> *"War driving is using a laptop's wireless NIC set in promiscuous mode to pick up unsecured WLAN signals. "*

The Service Set Identifier (SSID) allows a WLAN to be segmented into multiple networks, each with a different identifier. Each of these networks is assigned a unique identifier, which is programmed into one or more APs. To access any of the networks, a client computer must be configured with the corresponding SSID identifier for that network. Thus, SSID acts as a simple password, providing a measure of security. A weakness is that the SSID is widely known or shared and is easily obtained by freeware loaded onto a wireless network client.

Media Access Control (MAC) address filtering increases security by configuring an AP with a list of MAC addresses associated with the client computers that are allowed access to the AP. If a client's MAC address is not on the list, the AP will deny access. This method provides good security but is only suited to small networks. The labor-intensive work of entering MAC addresses and maintaining up-to-date lists on all of the AP devices obviously limits the scalability of this approach.

Wired Equivalent Privacy (WEP) minimizes the risk of radio frequency interception by somebody nearby. WEP is specified for encryption and authentication between clients and APs according to the 802.11 standard. WEP security is based on an encryption algorithm called RC4. The encryption algorithm is generated based on a key (a number sequence) entered and controlled by the user. All clients and APs are configured with the same key to encrypt and decrypt transmissions of data. WEP keys are 40 or 128 bits in length and can be configured in 3 possible modes: no encryption mode, 40 bit or 128 bit encryption.

An AP can be set up to provide encryption-only protection in open-system mode, or to add authentication in shared-key mode. MAC address filtering is often used together with this encryption. WEP security is best suited for small networks, as there is no key management protocol. As a result, keys must be manually entered into every client. This can be a huge management task, especially as keys should be changed regularly to provide a higher level of security.

As a more secure model, some vendors have developed VPN solutions that create a secure tunnel for your wireless traffic. An evolution of wireless security products now include the means to authenticate all wireless users before they can gain access to network resources, encrypt data as it prior to it passing through the air using the Advanced Encryption Standard and controlling user access to network segments through the use of policy servers.

Unusual Wireless Practices

Hackers are spending a good amount of time exploiting wireless networks. Hackers began "war dialing"--dialing phone numbers until they found an open modem--to access networks. The '90s Internet boom created easier and more direct avenues of attack, such as IP scanners and packet sniffers. Enter the next generation of network intrusion: war driving.

(Continued on page 7)

(Continued from page 6)

War driving is using a laptop's wireless NIC set in promiscuous mode to pick up unsecured WLAN signals. At this stage of the game, hackers are war driving--or "LAN-jacking," as it's sometimes called--wireless networks for anonymous and free high-speed Internet access. Wireless LAN war drivers routinely drive in their cars equipped with laptops loaded with a wireless LAN card, an external high-gain antenna and a global positioning system receiver. The wireless LAN card and GPS receiver feed signals into freeware, such as NetStumbler to detect access points and their identifiers along with their GPS-derived locations. A permutation of war driving is war flying where the vehicle is a plane instead of a car.

To mark AP locations, hackers use a technique called war chalking. They simple use chalk to place a special symbol on a sidewalk or other surface that indicates a nearby wireless network, especially one that offers Internet access. War driving and chalking are activities that can be thought of as counter cultural since the intended audience may not be to owner of the network that is targeted. A mainstream version of these ideas are called hotspots.

Hotspots are 802.11b-compliant public network nodes available to wireless users that are often located in heavily populated places such as airports, train stations, shops, marinas, conventions centers and hotels. Hotspots typically have a short range of access and are oriented on a specific geographic location. There are thousands of these locations that offer free or low-cost wireless access to the internet and network resources. Hotspots will change our culture by providing high speed internet access anywhere and at all the times.

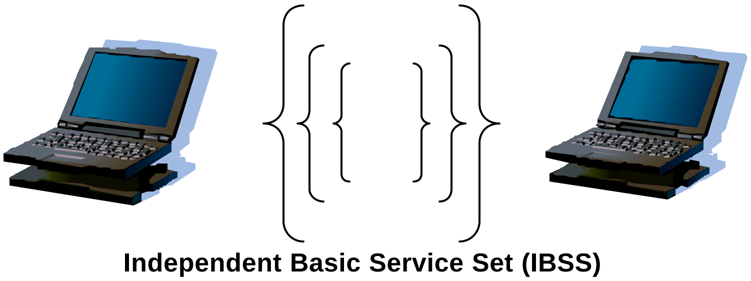


Figure 2: Ad Hoc Mode

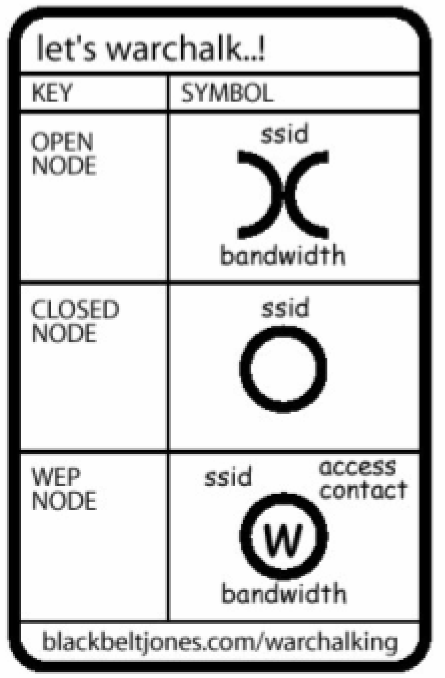
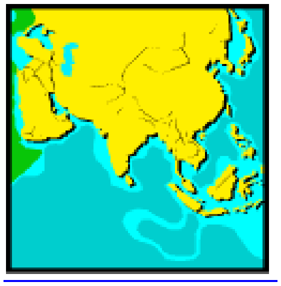


Figure 3: Warchalking symbols

Return to INDEX

Citizen-Centric E-Government in Asia

By Les Pang



The public sector in the United States can learn much from its Asian neighbors when it comes to transforming to a digital government. After all, Asian nations rank very high in terms of e-government leadership. For example, in 2001, Accenture ranked Singapore as Number 2 and Hong Kong Number 10 among the Top 10 e-Governments (U.S. is ranked 3rd).

Singapore defines e-Government as “a Government that recognizes the impact of ICT (information-communication technology) on governance in the digital economy, and exploits ICT in the government workplace and internal processes for the delivery of citizen-centric public services.”

Korea sees e-Government as transforming the nature of public service delivery by providing citizens convenience, effectiveness and efficiency never before possible. It creates the capacity to offer services to the public on an integrated, cross-agency basis therefore providing a networked government.

Japan views e-Government as the digitalization of central and local government, digitalization of public service, and providing relevant government information via the Internet.

Asian nations view e-Government as being beneficial in the following ways:

- Improves efficiency in public services and information delivery
- Stimulates cultural change within the civil service
- Facilitates the formation of public-private sector partnerships
- Improve competitiveness in the global marketplace

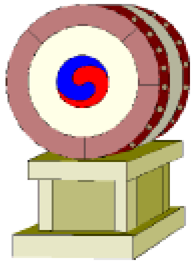
Technologies that enable e-Government in Asian countries include:

- Integration of front-end (citizen-facing) systems with back-end systems (internal operations).
- Wireless networks based on 802.11, Bluetooth and emerging 3G (3rd Generation) standards
- Digital convergence of television, personal computers and mobile phone for Internet access
- Web-based technologies including extensible markup language (XML) and content management
- Internet portals that serve as a window to a multitude of Government services
- Security technologies including public key infrastructure, encryption, and virtual private networks
- Electronic payment systems, imaging and workflow systems all aimed to improve government operational efficiency
- Smart cards for both authentication and stored-value purposes for citizens to perform secure and convenient electronic transactions

Examples of e-Government applications in Asia include:

- Education Administration Information Service (Korea) – supports access to a student’s record and permits the issuance of transcripts, certifications and other student documents all online
- Social Insurance Systems Interconnection project (Korea) - integrates health insurance, national pension, employment insurance and worker’s compensation data sources so that

There is a... ”movement towards ‘e-democracy’ – currently, most people see the citizen as the consumer and government as the provider of services; whereas ‘e-democracy’ is where one would perceive the citizen as a shareholder *and government as* a forum for setting policies.*”*



citizen data can be more accessible and updatable

- Management of government purchases using an ERP (Singapore) – joins together comptroller, logistics, accounting and treasury operations
- Home Tax Service (Korea) – supports electronic income reporting, tax notices and online payment
- Public Libraries (Singapore) – process redesign resulted in significant reductions in customer processing times
- Patent Online (Korea) – allows the online filing of patent and trademark applications and automates all of the in-house administration procedures and work flows
- Judicial Electronic Filing System (Singapore) – 75% of all court documents have been filed electronically by more than 320 law firms for rapid and secure access
- Juki Net (Japan) – a resident registration network system
- Government online citizen portal (www.ecitizen.gov.sg) which support multi-agency collaboration and Government-to-business portal (www.gebiz.gov.sg) which streamlines Government procurement procedures (Singapore)

Issues that concern Asian nations in implementing e-Government are as follows:

- Computer hacking and cyber terrorism – keeping government and citizen information safe
- Security management – making trusted transactions possible
- Data privacy – protecting personal information
- Interoperability – ensuring that a system can work with other systems without undergoing special efforts
- Governance – managing and controlling the e-Government infrastructure

Goals identified by Asian nations (particularly Singapore) for improving e-Government include:

- Applying customer segmentation (differentiating target groups of citizens)
- Increasing the depth of information
- Improving search capability
- Increasing integrated services ("thinking horizontally")
- Improving customization
- Increasing citizen space
- Increasing public-private sector partnership
- Using new enabling technologies

The future outlook for e-Government in Asia appears promising. Two key visions Asian countries have in this area are as follows:

- Movement towards "e-democracy" – currently, most people see the citizen as the consumer and government as the provider of services; whereas "e-democracy" is where one would perceive the citizen as a *shareholder* and government as *a forum for setting policies*. This infers a new and better channel for citizen participation in government activities. (E-voting is being implemented in Japan and online policy debates are held in Korea.)

- Bridging the digital divide and promoting equal opportunity – people who cannot afford computer technology and/or access, those who are not technologically adept, and those with physical handicaps all need to be part of the e-Government transformation and Asian countries are studying approaches to address this digital divide (Singapore is looking at providing broadband Internet access to *every* citizen).

As you can readily see, Asia has made significant strides in providing a more citizen-centric government by leveraging information technologies and new business processes and will do more in the future.

Source: 2002 Asia-Pacific CACS (Computer Audit Control Security) Conference Proceedings, September 2002.

A Quick Guide for Coping with Malicious Software

By Paul Flanagan

Malicious software or "malware" is a term used to describe destructive software programs such as viruses, worms, and Trojan horses. Generally, computer hoaxes and electronic-mail spam are lumped into this category. Malicious software can create great harm and expense (Computer Economics, a U.S.-based research firm, reported resulting costs of $11.8 billion). What should an individual do?

The first step is to perform some form of risk assessment. If you rely on e-mail, then you are clearly vulnerable to attacks. The extent of this vulnerability depends upon your own individual circumstances. Typically, the most significant risks are loss to your data and your precious time. Damage to your hardware and software is a possibility, but less likely. Still, ask yourself simple questions like: "How unpleasant would it be to miss a deadline because I had to recreate valuable data?" Or "what would be the impact on your work if the help desk staff had to reformat your hard drive and then reload your organization's standard software?" Are these risks you are willing to accept?

These types of questions should help you take the second step in confronting malicious software, that is, overcoming complacency. Realize that the true situation is when, not if, malicious software will adversely impact you. Once you come to this realization, then you are in the proper frame of mind to take the necessary precautionary measures. These measures include taking control of your data, investing in anti-virus software, and making a commitment to perform preventative steps needed to minimize the adverse impact of malicious software.

In taking control of your data, be honest with yourself and then be proactive. How much data do you save and how much of this data is truly necessary? Most people tend to be data packrats. They save documents, spreadsheets, and e-mail far longer than they really need because some day they might need them and they are not hurting anyone! At this point you may be tempted to ask: so what? After all, data storage is cheap and your time is valuable. You will get around to cleaning up your "my documents folder" or your Outlook Inbox some day. Unfortunately, unless you are the notable exception, some day never arrives. Your memory of the contents of each file grows dim and eventually you do not really know what data you really have nor where you stored it. The resultant excess of data and software may lead to personal calamity.

Do yourself a favor. Reserve a little time each week to examine the places where your data resides. If your organization has robust standard backup procedures, make sure you are using them regularly and properly. If your organization relies on you to take care of yourself, then do it. Eliminate unneeded data and software, and then protect what you do need by making systematic backup data files. Proper backups are relatively easy, cheap, and wise procedures.

Invest in anti-virus software. These products are cheap and readily available from commercial vendors. They work reasonably well as long as they are updated with the latest virus definitions. My observations over the last year indicate that vendors update the definitions several times a week. Knowledgeable people feel weekly anti-virus updates on personal computers are prudent.

Information assurance is a process, not a one-time event. Following these steps takes time. It may be inconvenient, and if you are not hit with malicious code it may seem unnecessary. Few people receive praise for preventing attacks of malicious software. You will have to draw solace from the fact that your preventive measures most likely saved you time, heartache, and the experience of being used as a poor example.

In summary, assess the risk to your computer and data. Overcome complacency -- the tendency to do nothing. Eliminate unneeded software and data. Invest in anti-virus software and keep it current. Stay the course and keep up to date with your stated preventative procedures. Being proactive will prevent you from being a victim of malicious software!

CobiT: Not Just Another Acronym (cont.)

(Continued from page 1)

- **Executive Summary** – consists of an Executive Overview Background and Framework, designed to provide senior management a succinct description of CobiT's key concepts

- **Framework** - illustrates and identifies IT business requirements for information through the introduction of high level control objectives

- **Control Objectives** - contain statements of desired results or purposes to be achieved by implementing the 318 specific, detailed control objectives

- **Audit Guidelines** – provides guidance for preparing audit plans and are linked to the control objectives

- **Implementation Tool Set** - describes practical approaches used by those organizations that quickly and successfully applied CobiT in their work environments.

CobiT looks at fiduciary, quality and security needs of enterprises; and provides seven information criteria (effectiveness, efficiency, availability, integrity, confidentiality, reliability, and compliance) that can be used to generically define what the business requires from IT. It is supported by a set of over 300 detailed control objectives.

CobiT, first released in 1996, is called an IT governance tool that has impact on how IT professionals work. IT governance is defined as “a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes.”

Now in its 3rd edition, CobiT has been implemented in over 100 countries throughout the world. It is based on 41 standards and best practices documents for Information Technology from standards setting bodies (both public and private) world-wide. These include documents from Europe, Canada, Australia, Japan and the United States.

The CobiT standard is supported by the IT Governance Institute which was formed by the Information Systems Audit and Control Association (ISACA), an organization having more than 160 chapters in over 100 countries around the world. The association exists to assist IT governance, control and assurance stakeholders deal with IT management, IT risk and IT process, and their interaction with corporate governance, corporate management, corporate risks and corporate processes. ISACA does that by providing value through various services, such as research, standards, information, education, certification, and professional advocacy. The Association helps IS audit, control and security professionals focus not only on IT, IT risks and security issues, but also on the relationship between IT and the business, business processes and business risks.

There are many reasons why an organization should adopt CobiT. According to ISACA, information technology clearly has a key role in corporate governance and management accountability. CobiT addresses this role by:

- Ensuring business-oriented solutions
- Serving as a framework for risk assessment
- Providing a means to communicate with management, users and auditors; and
- Having authoritative basis (internationally accepted, exhaustive, and constantly evolving)

Linking information technology and control practices, CobiT consolidates and melds standards from prominent global sources into an important resource for management, control professionals, and auditors. As such, CobiT represents an authoritative, up-to-date control framework, a set of generally accepted control objectives, and a set of audit guidelines.

CobiT helps by “ensuring business-oriented solutions serving as a framework for risk assessment providing a means to communicate with management, users and auditors; and having authoritative basis (internationally accepted, exhaustive, and constantly evolving).”

(Continued on page 12)

CobiT (cont.)

(Continued from page 11)

How IRMC Uses CobiT

The college uses CobiT as a best practices guide in its "Developing Enterprise Security Strategies, Guidelines, and Policies" (ESS) course. More importantly, CobiT is referenced in the General Accounting Office's (GAO) Federal Information Systems Control and Audit Manual (FISCAM) as a "generally applicable and accepted standard for good practices for controls over information technology." GAO uses FISCAM as their guide for reviewing information systems security. The ESS course covers CobiT and FISCAM in the same lesson so that students make the connection between these two methodologies.

Latest Developments with CobiT

A management and governance layer has been added, providing users with a toolbox containing:

- Performance measurement elements (outcome measures and performance drivers for all IT processes)

- A list of critical success factors that provides succinct non-technical best practices for each IT process

- A maturity model to assist in benchmarking and decision-making for control over each IT process

Among the current activities affecting the future of CobiT, two of them include:

- CobiTOnline – a web-based multi-user browsing, sharing and assessment tool which includes a repository of all knowledge relative to IT governance, performance measurement, control assurance, control objectives and practices

- CobiTLite – focuses on 15 most important processes and reducing the 318 control objectives down to 90

Because of the dynamic nature of information technology, CobiT is updated every 3 years. This will ensure that the framework remain comprehensive and relevant to today's business processes.

Conclusion

CobiT has been accepted in many organizations globally and new applications of this standard are being made every day. However, it should not surprise anyone that in those organizations where the CIO has embraced CobiT as a usable IT framework, this has come as a direct consequence of one or more CobiT champions within the audit and/or the IT Department. This framework is truly merits examination by any IT organization. Yes, CobiT is an acronym worth remembering!

Note: Dr. Robert Norris, Department Chair, Information Operations and Technology Department, has worked on the upcoming version 4 of CobiT as a subject matter expert.

Sources for More Information

For an executive overview of CobiT, visit:

http://www.isaca.org/exec1b.htm

You can download the entire CobiT open standard at:

http://www.isaca.org/ct_dwnld.htm

Reference: www.isaca.org

Here's Our Web Address!!!
http://www.ndu.edu/IRMC/techtalk_index.html
Check out our Previous Issues!

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/

**Department Chair: Dr. Robert Norris
Newsletter Editor: Dr. Les Pang**