Best Security Practices: Lowering Quality's Total Cost of Ownership in an Age of Growing Complexity

Title of Panel: Best Security Practices: Lowering Quality's Total Cost of Ownership in an Age of Growing Complexity

Panel Chair

James P. Craft, CISSP
Information Systems Security Officer (ISSO)
United States Agency for International Development (USAID)
1300 Pennsylvania Ave, Suite 2.12-032
Washington, DC 20523-2120
Voice: 202.712.4559
Fax: 202.216.3053
Email: jcraft@usaid.gov

Panelists

Tom Burke Director, Office of Information Security General Services Administration (GSA) 7th & D Streets, SW, Room 5060 Washington, DC 20407 Voice: 202.708.7000 Email: tom.burke@gsa.gov	Jack L. Brock, Jr. Director, Governmentwide and Defense Information Systems General Accounting Office (GAO) Washington, DC 20548 Voice: 202.512.6240 Fax: 202.512.6450 Email: brockj.aimd@gao.gov
Guy L. Copeland Vice President, Information Infrastructure Advisory Programs Computer Sciences Corporation (CSC) Room 621, VTC-B (M/C 315) Falls Church, VA 22209 Voice: 703.641.2561 Fax:: 703.849.1000 Email: gcopelan@csc.com	Robert E. Giovagnoni Executive Vice President for Strategic Relations Infrastructure Defense, Inc. (iDEFENSE) 6100 Lincolnia Road Alexandria, VA 22312 Voice: 703.914.9400 Fax: 703.914.7100 Email: rgiovagnoni@idefense.com

Session abstract

Best practices efforts have been typified by studies and published reports. They provided useful benchmarks to guide users embarking into areas of new endeavor. The CIO Council's Best Security Practices website takes this idea to a new level. The Federal government is facing enormous costs to secure its IT infrastructure. Avoiding some of these costs will take a new definition of best practices. The BSP website does this by capitalizing on the lessons of business process improvement and total quality leadership to approach security from a process perspective. Such a perspective is essential for performance measurement, results quantification, and costs assessment and reduction.

Brief summary of panelist's topics

Jack L. Brock, Jr.

"Fifth, agencies can expand on the good practices that they already have in place. Our audits have shown that even agencies with poor security programs often have good practices in certain areas of their security programs or certain organizational units. In these cases, we recommend that the agency expand or build on the practice throughout the agency. For example, one unit in one agency we recently audited had developed strong intrusion detection capabilities, but this capability was not being developed in other units of the agency. Once again, central coordination can help identify these pockets of excellence and ensure that their value is maximized on an agencywide basis." (Testimony before House Government Management, Information and Technology Subcommittee on 3/29/00, "Identify and Propagate Pockets of Excellence")

Guy L. Copeland

Greater sharing of information, including security practices, between industry and Government will require overcoming significant operational and legal impediments. Most notably, Government must assure industry that sensitive and proprietary information voluntarily shared with Government is protected from disclosure under the Freedom of Information Act. Additional concerns relate to liability, antitrust, security, regulation, and privacy issues. Each of these concerns may require legislation similar to the limited protection passed to limit liability for Y2K Information Sharing activities.

Robert E. Giovagnoni

According to the GAO, the National Infrastructure Protection Center (NIPC) was over 12 hours late in sounding the LoveLetter virus alarm. Apparently, a great deal of time was lost simply verifying the threat. By the time Federal agencies began receiving NIPC's warnings, the vast majority of them had already lost or defensively shut down all avenues of electronic communication. The paradigm needs to change. Rather than holding all communications for external validations, analysts, Government and industry, must work directly with computer scientists and senior engineers, i.e., share information, to deliver up-to-the-minute intelligence in real time. These immediate alerts ensure that all time-sensitive information reaches the hands that need it most, empowering them with intelligence, countermeasures, and solid, reliable counsel as to how best to, and cost-effectively, defend themselves.

Tom Burke

Not available at this time.

Background of audience

This panel will appeal to all Federal IT professionals both Government and vendors. Government is interested in making more cost effective decisions and deriving greater value from a shared knowledge resource. Vendors want to offer greater competitive value to their clients. The sharing of best security practices enables the entire value chain to flow more smoothly.

Best Security Practices: Lowering Quality's Total Cost of Ownership in an Age of Growing Complexity

by James P. Craft, Chair, Security Practices Subcommittee

January 17, 2000

In prehistory, the expansion of personal property spurred the invention and use of walls, vaults, locks, and seals. When you value something, you protect it. Today, with E-commerce, E-government, and IT-based critical infrastructures, the Federal government entrusts its information and business operations to its information systems, and often the Internet. With so much value online, the need for information systems security (ISS) becomes obvious to those who understand the threats to our systems.

Knowledge brings responsibility. That is why those of us who know the threats, and how to mitigate these threats, must find better ways to share this knowledge with those who don't.

Living as we do in a "Technology Intoxication Zone",[1] when ISS is mentioned, people think first of *technology* (e.g., firewalls, intrusion detection software, virus scanners). Technology is important to security but more important are the *practices of the people* who develop, evaluate, integrate, configure, maintain, and use that technology. Organizations can buy every available security product and still have insecure systems--if their people don't interact with the technology appropriately.

For decades the Government, especially DOD, led in ISS. If Government 'only *knew* what it *knows*',[2] that is, if it could only identify and reuse the best of its security practices, it would cost-effectively reap the benefits of improved security, protecting critical infrastructure. Government would then "serve as a model to the private sector on how infrastructure assurance is best achieved."[3]

To help make Government a model, the Federal CIO Council's Security, Privacy, and Critical Infrastructure Committee formed a Security Practices Subcommittee last October, giving Government, and perhaps the private sector, a way to share effective security practices. The subcommittee is delivering a draft plan for a Federal Best Security Practice Program and a proof-of-concept prototype for a Web-based Best Security Practice repository to the CIO Council at the end of this month. For a new Federal subcommittee, this is moving at relative light-speed.

The subcommittee has moved rapidly through teamwork and by reusing the results of previous efforts. Many Federal organizations, such as OMB, NIST, NSA, GSA, and GAO, shaped discussions of how to find and use best practices. Two efforts were especially important and were merged directly into the Security Practices Subcommittee:

---

[1] *High Tech, High Touch : Technology and Our Search for Meaning* by John Naisbitt, Nana Naisbitt, Douglas Philips, Broadway Books; ISBN: 0767903838, 1999

[2] See *If Only We Knew What We Know: The Transfer of Internal Knowledge and Best Practice* by Carla O'Dell and C. Jackson Grayson, Jr. with Nilly Essaides, The Free Press: New York, NY, 1998.

[3] Presidential Decision Directive (PDD) – 63, *Protecting America's Critical Infrastructures,* Critical Infrastructure Assurance Office

first, the NSA and NIST led PDD-63 Best Practices and Standards working group, second, was the US Agency for International Development's grassroots initiative, the Model ISS Program, which received help from the Government Information Technology Services Innovative Fund. Currently, the Security Practices Subcommittee has membership from over twenty Federal organizations.

The subcommittee addresses issues ranging from "What is a best practice?" to “How will the Government evaluate the Best Security Practices?” While some issues, such as the evaluation of practices, are scheduled for full resolution later, the subcommittee has reached consensus on core issues, such as definitions, initiative scope, and a standardized format for packaging security practices.

What makes this effort different from the many fine best practices initiatives that have gone before?

> ***First***, the subcommittee accepts that there may be alternate ways of accomplishing ISS tasks, such as network scanning. Alternate practices offer different strengths and weaknesses in terms of cost, speed of implementation, assurance, staff requirements, environment supported, etc. The term "Best" is often relative, determined by users needs. The subcommittee uses “Best Practice” as a term of art, as in industry, not as an ultimate ranking of goodness.
>
> ***Second***, the subcommittee accepts many ways of organizing practices. The subcommittee developed a baseline security process framework to organize practices, but also use a concept called multi-framework modeling that allows dynamic reorganization of best security practices under other models (e.g., OMB Circular A-130, NIST Special Publications, or the Systems Security Engineering Capability Maturity Model).
>
> ***Third***, and perhaps most importantly, the subcommittee focuses on reducing the Total Cost of Ownership (TCO) throughout a best practice's lifecycle. If best practices are not affordable, they are not usable. The subcommittee seeks to first collect the good and usable rather than wait for the perfect. The subcommittee seeks to reduce the TCO of security practices with many design and packaging features. This will lower documentation and maintenance costs to practice contributors while also reducing implementation costs to users. Increased quality and cost efficiencies will also come through continual process improvement of security practices using user feedback. Contributors and users both benefit.

Our current concept development phase is ending with the presentation of the draft plan and Web repository prototype to the CIO Council for approval by national leadership. With the next phase, Pilot Development, many new challenges begin. Where will the funding come from for program management, training, maintenance, and technical assistance? How will the Government measure the return on investments (ROI) and cost savings of Best Security Practice implementation? How will government partner with industry and give incentives to encourage the sharing of experiences, good and bad? How can this program support the new ISS and privacy legislation and the many existing and upcoming Federal initiatives?

There are many questions, but I believe that the subcommittee is on the right track. This is the greatest level of Federal interagency cooperation and willingness to innovate and implement ISS that I have seen in my twenty years of professional experience. If support of this initiative by groups, such as the Small Agency Council, the Federal Computer Security Managers' Forum, and the Information Technology Association of America continues, we all will succeed. If other communities of interest participate, such as the Chief Financial Officers and the Inspector Generals, the effect will be revolutionary. When this subcommittee succeeds in developing this cost-saving best practice methodology and infrastructure for ISS, the Government can apply it to the sharing of all IT practices. Thus, we will help reshape the future while saving hundreds of millions of dollars.

These are exciting times.

D. Short bio of panel chair and speakers

James P. Craft, CISSP (Panel Chair)

James P. Craft is the Information Systems Security Officer (ISSO) for the U.S. Agency for International Development (USAID). While at USAID, Mr. Craft initiated the Model Information Systems Security Program (MISSP), which was designed to collect, organize, and disseminate best security practices (BSPs) for civil departments and agencies. In October 1999, he was asked to chair the Chief Information Officer (CIO) Council's Security Practice Subcommittee (SPS). In support of the SPS, USAID developed a proposed program plan for a Federal BSP Program (FBSPP) along with a prototype proof-of-concept web repository (http://bsp.cio.gov). Previous to USAID, Mr. Craft was employed by SRA International, Inc., Booz Allen & Hamilton, BETAC,Inc., and the U.S. Marine Corps. He earned a Business Management degree from George Mason University in 1978. Mr. Craft has received the CIO Council's 1999 and 2000 Technology Leadership Certificates, the 1999 USAID Office of Inspector General (OIG) Annual Achievement Award, and the National Security Agency's Annual SSE-CMM Program Achievement Award in 1999.

Jack Brock (Panelist)

Jack Brock is the Director of the Governmentwide and Defense Information Systems Issue Area at the U.S. General Accounting Office. Mr. Brock is responsible for information management evaluations at the Departments of Defense, State, Justice, and the Treasury and NASA. He is also responsible for developing guidance for improving such areas as performance management and investment controls. Additionally, Mr. Brock is responsible for governmentwide reviews of computer security issues and critical infrastructure protection issues. He has testified before Congress on numerous occasions on these topics and is heavily involved with the computer security community to improve government's responsiveness to computer security threats. To this end, Mr. Brock's issue area has developed guidance for improving management responsiveness to security threats. This guidance—based on a study of leading organizations—has been endorsed by the Federal CIO Council and adopted by several federal agencies. Mr. Brock joined the General Accounting Office after receiving his Master of public administration degree from the University of Texas at Austin. He is also a graduate of the Harvard Business School Program for Management Development.

Tom Burke (Panelist)

Mr. Tom Burke, Assistant Commissioner for the GSA, FTS, Office of Information Security, has over 32 years experience in the Information Security arena. He is an active participant on the National Security Telecommunications and Information Systems Security Committee (NSTISSC), Military Communications Electronics Board and various CIO Security Committee Groups. Tom also serves as the Chief Infrastructure Assurance Officer (CIAO) for the General Services Administration and is the Executive Agent for the Federal Sector in the implementation of PDD-63.

Guy L. Copeland (Panelist)

Guy L. Copeland represents CSC's CEO in the President's National Security Telecommunications Advisor Committee (NSTAC), an advisory body which provides

industry advice regarding critical, information and telecommunications services supporting our national economy and other critical functions of society. He also co-chairs the Best Practices Subcommittee of the Communications & Information Working Group (CISWG). Prior to joining CSC, Mr. Copeland's Army career included research and development projects, directing organizations responsible for fielding, operating and maintaining communications systems, and a tour in Vietnam as a helicopter pilot. In 1983-84, he was a Congressional Science Fellow in the office of Senator John Warner (R, VA). Mr. Copeland is a member of the Advisory Board for "IT Professional," a new publication of the Computer Society of the Institute of Electrical and Electronic Engineers. He received the 1999 Award for Excellence in Information Technology from the Armed Forces Communications Electronics Association International.

Robert E. Giovagnoni (Panelist)

Robert E. Giovagnoni has been intimately involved in the government's efforts on critical infrastructure protection and is recognized at the highest levels of the federal government as a legal expert on computer crime and cyberspace law. He came to iDEFENSE from the Critical Infrastructure Assurance Office (CIAO), where he served as General Counsel and Assistant Director. He helped organize the President's Commission on Critical Infrastructure Protection and served as General Counsel to the PCCIP and its Transition Office, both predecessors to the CIAO. He was a key author of Presidential Decision Directive 63, Protecting America's Critical Infrastructures. Giovagnoni holds a Bachelor of Arts degree from Manhattan College, a Juris Doctorate from St. John's School of Law, and a Master's of Law degree from the University of Missouri at Kansas City.