WHO SHOULD REALLY MANAGE INFORMATION SECURITY IN THE FEDERAL GOVERNMENT

Alexander D. Korzyk, Sr.
Department of Information Systems
Virginia Commonwealth University
A. James Wynne
Department of Information Systems
Virginia Commonwealth University

KEYWORDS: Information System, CIO, Internet, World Wide Web, Computer security

ABSTRACT

The importance of security technology to the government organization was documented in a 1996 survey of all the new Federal Chief Information Officers conducted by the Environmental Protection Agency three critical technologies stood head and shoulders above the rest. Over half of the CIOs selected these three closely related critical technology challenges facing the new Federal Chief Information Officers.

- The f**irst** critical technology on the list is the Internet Worldwide Web and organizational Intranets. These relatively recent technologies are redefining business processes in corporations and in those corporations that re-engineered more than a year ago. Unfortunately, the government and corporations have not fully embraced the impact of this first critical technology because of the second critical technology.
- The **second** critical technology is security technology. Organizations and corporations at all levels of management have never placed a high priority on information security until the last two years. During the Cold War the Department of Defense, National Security Agency, Central Intelligence Agency, and the Federal Bureau of Investigation enforced strict information security requirements. However, now there are literally millions of organizations and corporations that want to participate on the World Wide Web but are afraid to do so because of the lack of security in their communication's infrastructure and information systems. Until only recently most of these organizations had operated in isolation on their own private networks. Now as budget cuts become commonplace and organizations want to enter the World Wide Web without compromising information security, where everyone's information becomes available to everyone else if it is not protected properly. Similarly, the government and private corporations have not fully embraced the third critical technology because of the second critical technology.
- The **third** critical technology is Electronic Commerce/Electronic Data Interchange (EC/EDI). The government and corporations have again been hesitant to implement EC/EDI because of the lack of security technology used on the Internet and World Wide Web. Government and private industry want to use the Web as the infrastructure on which to run EC/EDI. The majority of CIOs agree on the challenges, but are these the individuals who should be responsible for ensuring organizational communications and information security? Should the lackadaisical managers who ignored security technology for years manage security technology? Will the CIO be impartial enough to not compromise security while facing deadlines and pressure from the CEO or agency head? This paper addresses the question of who should really manage security technology for government organizations and presents the basis for developing a business model for managing security technology.

Introduction

Massive amounts of changes in technology and its uses are occurring at an alarming rate. Since the end of the Cold War in 1989, after Desert Storm in 1991, and the election of President Clinton in 1992, sweeping transformations in government operations have taken place at the local, state, and Federal level of government. Along with the shifts in how governments operate, dynamic advances in commercial technology have acted as catalysts for changing the business processes of government. These processes depend more and more on enabling information and security technologies. In two years personal computer central processing units have moved from an Intel 486-33 megahertz chip to an Intel Pentium II 300 megahertz chip with a 64-bit bus architecture. Workstations and mid-range computers have advanced from single RISC-based chips to symmetric multiprocessor RISC chips. Networks have evolved from mainframe centric to distributed client/server and peer-to-peer architectures.

Communication mediums have moved from copper-based Ethernet to fiber optic based frame and cell relay, SONET, FDDI, and ATM protocol. Transmission speeds have increased by an order of magnitude to over 100 megabits per seconds. The Internet has grown from a few hundred thousand users to over 100 million users. The management of these revolutionary and fast-developing technologies has also undergone major changes. The American public as primary customers of the Federal agencies is taking charge [13]. Efforts to reengineer the Federal government, particularly the Department of Defense (DOD), have stagnated in recent years, but are now getting more attention as Congress gets serious about streamlining and cuts budgets [15]. The passage of the Clinger and Cohen Bill forced major federal agencies to appoint Chief Information Officers to replace the senior information resource manager. This paper examines the constantly changing, and evolving new roles of government officials in managing information and the security of that information in the "Information War" and offers recommendations for challenges for managing security in this new environment. The winners will be those who gain dominance through information [7].

CIO Challenges and Critical Technologies

The Association for Federal Information Resource Management conducted a Top Ten Challenges Survey of the Federal Chief Information Officer in October 1996. The survey findings present and discuss the top 10 challenges facing CIOs today as defined by a number senior information technology officials and managers at Federal agencies and departments. Table 1 lists the top ten challenges considered to be the most important to the Federal CIO [2].

Table 1. Federal CIO Top 10 Challenges

Number	Challenge	Rank by Percent
1	Implementing IT capital planning and investment management	76
2	Measuring IT contribution to mission performance	56
3	Formulating or implementing an agency IT architecture	52
4	Aligning IT and organizational mission goals	41
5	Championing BPR as a precursor to IT decisions	37
6	Building effective relationships with agency senior executives	35
7	Gaining a seat at the senior management table	32
8	Engaging senior executives on IT strategic directions	30
9	Providing effective IT infrastructure and related services	27
10	Ensuring Year 2000 operations	25

The first three challenges in Table 1 directly affect the three critical technologies identified as most important in Table 2 which lists the most critical technologies considered to be most important to the Federal CIO in performing the CIO function during the years ahead. Table 2 lists the top ten critical technologies from the survey [1].

Table 2. Federal CIO Top 10 Critical Technologies

Number	Critical Technology	Rank by Percent
1	Internet/Intranet/Web	73
2	Security Technology	68
3	Electronic Commerce/Electronic Data Interchange	57
4	Distributed Computing	47
5	Data Warehousing	42
6	Client/Server Computing	41
7	Workflow	35
8	Executive Information Systems/Decision Support Systems	28
9	Groupware	22
10	Relational Databases	21

Who Should Manage Information In The Federal Government?

Governors, Senators, Representatives, and officials at all levels of government organizations, as well as corporations, did not consider information as a valuable resource in the early 1980s. These managers of government and corporate employees did not consider knowledge capital (the knowledge of their peers and subordinates) to be of value [26]. The only valuable knowledge was that which affected national security. The government at the national level focused all efforts on defeating the Soviet threat. By the mid-1980s, senior executives recognized that computer information could be very powerful if used correctly. Federal agencies sent information resource managers to the Information Resource Management College in Washington, D.C. for a quick four-month course on how to manage information. Industry followed suit by creating a Chief Information Officer position. Unfortunately, for both government and commercial information managers, most of the CIOs did not sit on Executive Boards even though they had significant leadership responsibility for information system projects that required executive sponsorship from board members [4]. In private industry information managers typically reported to the Chief Financial Officer who was a participating member on the board. In the government they typically reported to the resource manager who also controlled finance. Industry is now beginning to redefine the role of the CIOs by replacing them with Chief Technology Officers (CTOs) [3]. The Federal Government is just now beginning to get rid of their information resource manager position and replace them with CIOs [23].

Who Should Manage Security In The Federal Government?

Security consists of more than one type of security. Typically security consists of physical security, procedural security, computer security, operational security, personnel security, communications security, and information security. Before the recent flood of Internet users, information security had often taken a low priority compared to operational security. Security guards watched building entrances and exits, installed video cameras to monitor hallways, stairways, etc. to reduce the number of security personnel needed to physically secure a building. Managers considered locked drawers and a locked room secure. General managers were responsible for their organizations to follow the security regulations written by military intelligence personnel and the National Security Agency. Only classified information received any large amounts of capital to protect it from threats.

In the mid-1980s, security specialists decided that since there were so many computers emanating electromagnetic waves, that there was no way that a spy could zoom in on the signature of any one personal computer and collect data because of number of cross overs between personal computers. Thus, the elimination of the TEMPEST individual workstation electronic shielding requirement saved the Federal government millions of dollars and allowed the Federal government to buy personal computers off-the-shelf. The number one challenge for Federal CIOs from Table 1 is implementing IT capital panning and investment management across the agency. Who should decide on how much to spend on security technology capital required to make the Internet/Intranet/World Wide Web secure for EC/EDI?

Managers did not consider other information valuable enough to protect it with other than minimum protection. Most unclassified systems operated at great risk since the managers typically felt that the unclassified information could not be harmful to the national interests of the United States. This perspective has changed drastically. Information aggregation has become a critical topic because highly summarized data may reveal significant amounts of information about an organization, country, corporation, etc. [14]. In 1989, the Department of Defense recognized the onset of the “Information War” and began to take steps to prepare for it. DOD issued a memorandum mandating that all unclassified systems comply with the National Computer Security Evaluation Criteria level C2 by the end of 1992. Unfortunately, four years after that date most services are still working on meeting that goal due to high costs and extremely complex solutions. A new doctrine of warfare called “Information Warfare” is sweeping through DOD forcing great changes to how business is conducted [7]. This is placing even more pressure on the services to reach the C2 goal. Simply protecting the gateway to the system from external threats is extremely shortsighted. Most attacks on information systems come from within the organization by an insider. Reaching the C2 level will help contain the amount of damage an insider can wreak.

The Information Technology Management Reform Act (ITMRA) of 1996

The Information Technology Management Reform Act (ITMRA) established a focal point for information technology and information resource management issues. The significance of ITMRA was to mandate the appointment of a CIO by each Federal agency. Thus, the passage of ITMRA established a new framework for strategic management of information technology by the Federal government. CIOs would now be the focal point for managing information technology in the future [1]. However, the Office of Management and Budget (OMB) took over control of all Federal CIOs from the General Services Administration (GSA). Previously, GSA had provided oversight responsibilities for all Federal Departments and Agencies to include spending authority. Specifically, the deputy director of OMB, has become the chairman of the new Federal CIO Council. This replaced the Industry Advisory Council of which senior information resource managers were members.

The new CIO Council will not be the principal forum for making decisions or setting policy. Rather, the CIO Council will be the principal forum for generating ideas and sharing best practices or even using the best practice of another agency by cross leveling. Although the Deputy Director stated that OMB will not take over programs, OMB will realign budgets to force agencies and departments to make necessary changes whenever the agency or department goes more than 10% over their budget [22]. ITMRA's directing the 23 largest agencies and departments to replace their senior information resource management positions with Chief Information Offices will involve a cultural change because managing information technology will be a strategic function instead of a support function. ITMRA created an environment for change by establishing a CIO position, which will work with senior management and provide information technology solutions to the business of the organization [24]. So far, most of the agencies and departments have complied by simply changing the title of the senior information resource manager to Chief Information Officer. Some of the CIOs are political appointees and some are government civil service careerists. Some have information technology experience where others do not. In all cases, the CIOs are all responsibilities listed in Table 3.

Table 3. CIO Responsibilities

No.	CIO Responsibility
1	Formulating agency information technology investment strategies
2	Integrating IT operations with core programs and budget plans
3	Identifying interagency system development opportunities
4	Developing and implementing the organization's information architecture
5	Establishing, staffing, and professional development of all IT personnel
6	Devising performance metrics for evaluating IT investments and system results

The second major mandate of ITMRA was the repeal of the Brooks Act. The Brooks Act was thirty years old and controlled the management of Federal information technology. The primary problem of the Brooks Act was the Delegation for Procurement Authority, which created a huge bureaucracy in all agencies.

The Federal CIO

One of dangers of placing the responsibility of managing security technology with the Federal CIO is that they may be a political appointee instead of a careerist. This could be an advantage to the organization, which has a political appointee. Coming from industry or academia, the appointee will have key contacts that could sway the amount of the IT budget approved for that particular agency or department. A careerist CIO, particularly one who has been in the government for over ten years, would not have the comprehensive political contacts, and would only add another layer to the bureaucratic structure without being effective. An appointee would be much more familiar with the capital investment process used by corporations for IT and may have a better chance of being successful than a federal careerist CIO. There is no organizational model for determining to which the CIO would report. ITMRA deliberately left some ambiguity in the bill to allow agencies and departments the flexibility to establish their own reporting chain. Industry does not follow any particular model because there is no formal CIO model [8]. Many corporations follow the old MIS model because they simply renamed the vice president of MIS or information systems director as CIO [24]. Similarly, the Federal CIOs will probably follow the same senior information resource manager model and simply rename the position as CIO as in the case of the Department of Defense. The Office of Management and Budget will take the place of the GSA in providing oversight of IT acquisitions in the Federal government. In that vein, they are focused on the location of the CIO office, the duties of the CIO, and the qualifications of the CIO [20]. The CIO office location should be no less than one level down from the Secretary or Director of a bureau and that the CIO not report to the CFO.

The Federal Chief Information Security Officer (CISO)

The Gartner Group and others have argued for some time that the head of corporate information resources security should be elevated to at least the same level, yet separate from the CIO, or better yet upgraded to the same level as the CEO and the CFO. All of these positions would report to the Board of Directors [17]. Table 4 shows the CISO paradigm.

Table 4. CISO Paradigm

Change Elements	Security Culture	Actions
Information Security Model	Business Risk Management	CISO Office
Information Security Programs acceptance and creditability	Fundamental Behavior by entire organization	Business Information Security Officers
Link to Business Objectives	Infrastructure Cornerstone	Sell Security

The CISO must be able to communicate with management in common business terms. Communication should occur not just in business meetings and via electronic mail messages, but also in a formal security bulletin for executives whose lower level managers have reviewed prior to it being sent to upper management. The CISO must be an advocate in the security technology industry. Information security may be designed into a commercial product but the system administrator does not implement the security features or configuration because it requires much more knowledge of the information system. For example, both HP UX and Microsoft Windows NT provide significant security protection. However, none of the security features are enabled when the product is first installed! Trusted facility manuals for the system administrator are necessary to explain how to enable security.

The world of security has always required independent verification and validation for classified government information systems. The CISO could provide that independent verification and validation for both corporations and government organizations. If management allows the CIO to manage information security, the independent verification and validation may not get performed properly because of internal pressures to get products delivered even if it means short cutting security. Any other position would also have biased internal pressure.

The Federal CEO

The Federal government has many Presidential Cabinet Officers who are the CEO of their respective organization, e.g. the Secretary of Defense, the Secretary of State, etc. There are agency heads who are not Cabinet Officers but who are political appointees, e.g. Director of the Federal Bureau of Investigation, Director of the Central Intelligence Agency, the Director of the National Security Agency, etc. As demanding customers have changed the focus of the corporate world, there has also been the rise within the government sector by the demanding customer [19]. Government customers don't care about the structure and organization providing the service. They only care about results and value [12].

The National Aeronautic and Space Agency has created better value for its customers and greater opportunities for their employees by outsourcing the space launch program to private industry and concentrating on what it does best, research and development. NASA is a classic business example of an organization redefining its purpose, getting back to its core competency, and allying itself with outside experts [5]. Customer-oriented public organizations still face penalties and punishments such as being caught up in the 25% across-the-board budget cuts over the next five years [19]. Even though agencies and departments reengineer, in the context of government, reengineering becomes synonymous with downsizing. Vice President Gore is in charge of the Reinventing the Government Program. In other words, reinvention means continuing to provide the same level of service after drastic budget cuts [5]. Another agency leading the government reinvention movement is the Internal Revenue Service as part of the Department of Treasury. The IRS is redesigning its core business processes and aligning its modernization investments with the business strategy. To date, the IRS has spent $2.8 billion on the tax modernization system with little to show for the $2.8 billion dollar investment, other than soft development [6].

The IRS business case includes:

1) Declining budgets, but pressure to increase productivity;
2) Difficulty meeting expanding workloads;
3) Intensified external oversight;
4) Increasing inability to respond quickly to congressional and executive orders;
5) The need to provide constituents with service and technology options provided in the private sector; and
6) Outmoded technology.

Perhaps the agency with the most at stake is the Federal Aeronautics Administration with the Air Traffic Control System to operate. Most of the rest of the world has already privatized their air traffic control systems. Federal CEOs face even greater pressure from the public to reengineer their decades old systems no matter what agency or department they lead.

The Federal CTO

Since security is considered a separate technology from information technology it makes sense to have a Chief Technology Officer. Industry has already recognized that the role of the CIO may be waning [3]. With the call by the Technology Officer to "Don't automate. Obliterate!" [11], there have been tremendous power struggles occurring in industry between the CIO and the individual in charge of business process reengineering. CIOs who have not made a significant contribution to the bottom line of the corporation find themselves fired or relegated to an insignificant project waiting to retire. Ford Motor Co. recently eliminated the CIO position completely. The CIO became totally ineffective because of an aggressive reengineering team and a high tech skill deprived IS division. In fact, a Ford spokesman said, "We reduced one layer of management by getting rid of the CIO position." [3]. If the CIO is part of the problem, then perhaps the solution in the Federal government would be to establish the Chief Technology Officer (CTO), who is often called the Scientific Advisor. This person is now in charge of security technology. The Scientific Advisors do not report to a CIO. Insteadt, they report directly to the CEO as Vice President and Technology Officer [10]. The Federal CTO would have a global view of the technology that the organization uses. A Federal CIO could not handle keeping up with the fast paced changes in technologies. Having the CTO report to the CIO would only add another layer of management and stifle creativity by preventing the creative uses of new technologies.

The Federal Senior Information Resource Manager

Over the past ten years the effectiveness of the federal senior information resource manager has eroded. Many of them are responsible for accrediting information systems to operate in their agencies. The pressure of fielding information systems on time has increased each year while many agencies have continued to fail to meet production schedules. These accreditation authorities have had short political lives and most often traded security for getting the product completed faster with lots of risks. By the time the system became operable in the agency, the accreditation authority would no longer be at that organization because they would take the credit for developing the system and try to get promoted immediately.

The organizational culture of federal bureaucracy is rampant with managers at all levels avoiding blame and responsibility, treating co-workers as competitors, feeling entitled, and not feeling intense and committed [12]. Protocol and work rules made by bureaucrats, lucky enough to move up the hierarchy ladder, frustrated inventiveness. These managers felt so secure in their positions, i.e., that no matter how bad they performed their jobs, they would not get fired. They would simply get moved to another position and sometimes even get promoted.

In the past three years, the Federal government has reduced its size by over 700,000 personnel with no replacements. Over 500,000 personnel came from reducing the armed forces or the Department of Defense after the Cold War and Operation Desert Storm in 1991. Congress has mandated further cuts of the government civilian workforce by 1999. Since security and stability of Federal government civilian personnel is no longer assured, the chances that a bureaucrat will be able to accomplish any of the challenges in Table 1 or implement the critical technologies in Table 2 are very remote.

In a recent study of a Federal Installation CIO, the government had contracted most of the work on a global scale [25]. The CIO had direct control of only 75 employees out of a workforce of 1275 employees. There was a dual chain of command for the government and the contractor. The government employees essentially performed no productive work. They simply pushed paper required to keep the contractors employed. The CIO had to manage with unclear lines of responsibility because of matrix support and the slow technology acquisition process. This CIO spent over 70% of the workweek in meetings and 30% on deskwork and phone calls [25]. Most of the meetings were with contractors, not government personnel. However, the CIO operated as if the contractor personnel worked for him just as the government personnel. Making the senior information resource manager the manager for security technology would only create another contractor position to actually do the work and another government position to write up the task order on the contract for the contractor to do the work.

Who Should Manage Information Security In The Federal Government?

The Federal government is a unique, multifaceted organization. Over 40 of the 50 states of the United States have had a CIO for several years. In fact, all the states whether they have a CIO or senior information resource manager meet annually to discuss their successes and failures. The authors propose that ITMRA should not try to develop models completely based on industry practices, rather, ITMRA should take the lessons learned by the National Association of State Information Resource Executives and combine them with traditional business school models. Each state is a microcosm of the United States. Information technology has been a high priority for some states for several years whereas other states have yet to begin to use recent information technology. The main reason to have a CIO is to focus responsibility, i.e., have someone to shoot when things go wrong [16]. The most common reason state government CIO positions have been created is that a large development project has failed or has run far overbudget or overschedule. A scapegoat is convenient but the state government CIO position generally does not result in the efficiencies and economies the private sector expects from their CIOs. Whereas, the state of North Carolina provides a good CIO model, IOWA does not have a CIO. Just like the 50 different states, each agency will probably end up establishing its own structure. Some Federal CIOs will report directly to the secretary and others will report to a CFO.

Without a model to follow and no one to require compliance with the way in which security is enforced, there is no way to predict what will happen. In a bureaucratic organization such as the Federal government, the best way to implement a strategy to manage information security is to appoint a Chief Information Security Officer. The CISO understands that as information systems pervade the organization, the complex protection of those systems become more dependent upon systemic perception than security technology [27]. Even though, the individual may not have great technical knowledge or too much authority in some cases, at least everyone in the agency knows who is responsible for information security and who to call about information security.

Conclusions

Most federal agencies could not tell investigators who is responsible for computer security at their agency [9]. Giving the CIOs responsibility for information security would only add more confusion to enormous amount of challenges they face. CIOs will have a conflict of interest if the person in charge of information security reports to them. As this paper has shown the security threat is one that needs to be taken seriously by whoever is in charge of information security and not diminished by a CIO intent on meeting a scheduled production date. The CEO does not have the technical expertise to make a security technology decision, let alone any technology decision [18].

Assigning the CTO responsibility for information security, like the CIO, would only add more confusion to the challenges of technology changes. CTOs will have a conflict of interest if the person in charge of information security reports to them because they may favor a different type of security solution that costs less so they can have more funds for pet technology projects. Certainly, the solution does not lie with the anorexic dinosaurs called senior information resource managers since they are the responsible party for failing to plan and design for information security in the first place. Thus, the most logical and best position to manage information security and security technology is the Chief of Information Security Officer. This position should report directly to the CEO to ensure that no conflict of interests exists at the lower executive management level and by reporting to the CEO, information security will be perceived by everyone as important because the CEO reviews it. Best of all, employees at Federal agencies would be able to tell anyone who is charge of information security.

Recommendations For Further Research

The Software Engineering Institute and the Federal government developed the Capability Maturity Model for software development. The development of an Information Security Capability Maturity Model is a great opportunity for further research.

The National Association of State Information Resource Executives could supply data for the past ten years when the first state appointed a CIO. The authors did not find any references, which used any data from NASIRE.

A study of state government CIOs to help develop the proposed Information Security Capability Maturity Model needs to be conducted.

References

[1] The Federal Chief Information Officer, A Seat at the Table, Association for Federal Information Resources Management, June 1996, p. 9.

[2] The Federal Chief Information Officer, Top Ten Challenges Survey, Association for Federal Information Resources Management, October 1996, p. 3 and 14.

[3] Ford Retools, by Doug Bartholomew, Information Week, April 1, 1996, p. 14-15.

[4] Trends in Information Services: 1995, by George H. Bodnar, Internal Auditing, Spring 1996, p. 64

[5] Better Government, Not Necessarily Smaller, by James Champy, Government Executive, September 1996, p. 7A.

[6] The Mess At IRS, by Edward Cone, Information Week, April 15, 1996, p. 40.

[7] The Air Force Software Perspective, Crosstalk Journal of Defense Engineering, October, 1996, pp. 3 and 5.

[8] The Era of the Federal CIO, Continuing the Partnership, interview of Lorraine H. Fenton, CIO, IBM North America, Industry Advisory Council, Federation of Government Information Processing Councils, September, 1996, p. 6.

[9] Only slight improvement seen in security of federal and corporate systems, by Nancy Ferris, Government Computer News, June 24, 1996, p. 13.

[10] Net pioneer: Intranets ahead of their time, An interview with Jerrold Grochow, Government Computer News, Nov. 4. 1996, p. 20.

[11] Reengineering Work: Don't Automate, Obliterate, by Michael Hammer, Harvard Business Review, 1990.

[12] The Soul of the New Organization, by Michael Hammer, Government Executive, September 1996, p. 2A.

[13] Reengineering The Corporation, A Manifesto For Business Revolution, by Michael Hammer and James Champy, Harper Business, New York, NY, 1993, 3 rd Ed., p. 18.

[14] An "Events" Model For Information Aggregation, Journal of Computer Information, Winter 1994-1995, p.

[15] A Vision Too Grand, by Heather Hayes, Government Executive, February 1996, p. 26-29.

[16] CIO exists to be a scapegoat, one rueful veteran claims, by William Jackson, Government Computer News, June 24, 1996, p. 72.

[17] The Second Annual Information Security Conference Report, by M.R. Kabay, National Computer Security Association News, July, 1996, p. 25

[18] Technology Decisions: CEOs Take The Wheel, by John Kador, Beyond Computing, January/February 1996, p. 50-53.

[19] A Soul Divided, by John Kamensky, Government Executive, September 1996, p. 6A.

[20] The Era of the Federal CIO, Continuing the Partnership, interview of John A. Koskinen, deputy Director, OMB, Industry Advisory Council, Federation of Government Information Processing Councils, September, 1996, p. 9.

[21] Third Annual Iway Poll: Web presence is the point, InfoWorld, Dec. 23/30, 1996, p. 1 and 12.

[22] Agencies Grapple With Who's In Charge of IT, by Kevin Power, Government Computer News, Sept. 9, 1996,p. 1 and 101.

[23] Survey Reveals The Challenges CIOs Face, by Kevin Power, Government Computer News, October 21, 1996, p. 1 and 62.

[24] Information Systems Management In Practice, by Ralph H. Sprague, Jr. And Barbara C. McNurlin, Prentice Hall, Englewood Cliffs, New Jersey, 3rd Ed., p. 37.

[25] The Nature of Information Technology Managerial Work, The Work Life of Five Chief Information Officers, by Charlotte S. Stephens, Quorum Book, Westport Connecticut, 1995, p. 79.

[26] The Value of Computers, Information, and Knowledge, by Paul A. Strassmann, URL—http://www.strassmann.com/pubs, January 30, 1996, p. 11.

[27] Computer Security Within Organizations, by Adrian R. Warman, The MacMillan Press LTD, London, England, 1993, p. 143.