Naval War College Review

Volume 54
Number 3 *Summer*

Article 11

2001

Set and Drift: The Perils of Paperless

Patrick J. Geary

THE PERILS OF PAPERLESS SOME QUESTIONS ABOUT THE LATEST DEFENSE BUSINESS TREND

Patrick J. Geary

In a document released in November 1997, *Defense Reform Initiative: The Business Strategy for Defense in the 21st Century*, then–Secretary of Defense William Cohen stated, "To carry out our defense strategy into the 21st century with military forces able to meet the challenges of the new era, there is no alternative to achieving fundamental reform in how the Defense Department conducts business."[1] One initiative spelled out in the document concerns how Defense Department business practices are related to the management of technical data supporting defense weapons systems.

Citing how recent improvements in information technologies have allowed the business world to conduct numerous operations in a paper-free environment, Secretary Cohen brought attention to the need for the Department of Defense (DoD) to move in the same direction. This department-wide initiative calls for 85 percent of all DoD technical manuals and 80 percent of all technical drawings to become electronically accessible. It is designed to achieve significant benefits: "By integrating paperless technical data management with electronic commerce for business information, DoD will eventually be able to support all major weapons systems in a paperless environment, from the initial design phase through production, operation, and maintenance."[2]

If fully implemented, the initiative promises such specific benefits as: a reduction in the cycle time for production contract awards; a reduction in the time to review technical drawings; a reduction in the number of contract data requirements lists needed to conduct business with DoD program offices; and significant cost avoidance.[3]

Patrick J. Geary is currently the Technology and Force Protection section head for the Naval Sea Systems Command, Washington, D.C. He received a bachelor's degree from Virginia Commonwealth University. Mr. Geary is a June 2000 graduate of the Naval War College, where he earned a master's degree in national security and strategic studies. He also holds a master's degree from the University of Richmond.

Mr. Geary is the ninth national president of the Operations Security (OPSEC) Professionals Society.

Naval War College Review, Summer 2001, Vol. LIV, No. 3

Despite these potentially significant benefits, however, the conversion of tens of millions of technical drawings, models, manuals, and manufacturing information into electronic images for easier access has profound implications for the adequate protection of the nation's most critical and sensitive defense-related information. Two primary concerns are access control to proprietary information and protection of classified information. Without addressing these issues fully, DoD's "new business strategy"

might very well have an overall negative impact on U.S. national defense strategy.

PROPRIETARY INFORMATION

Defense-related technical data includes a variety of sensitive (and sometimes classified) information that must receive limited distribution and careful access control. Protection requirements for this information are specified in federal statutes and regulations, as well as directives, instructions, and standards of the Department of Defense, each of the military services, and the Department of Commerce.[4] One type of sensitive data requiring protection from unauthorized disclosure is proprietary information. There are three main concerns with electronically accessible proprietary information: legal liability, labeling and controlling the accuracy of data, and identifying users.

Recent federal court decisions, such as *Bernstein v. U.S. Department of State*, and subsequent written opinions from legal counsel of the Department of the Navy have focused on the need to protect proprietary data from unauthorized access via the Internet.[5] This legal issue has significant implications for systems that will operate and interface via the Internet. These legal interpretations have specifically stated that failure to properly protect proprietary data could result in violations of federal statutes such as 18 USC 1905, which prohibits the disclosure of proprietary data by the federal government.

The legal issue involving proprietary information is especially complex. Much of what the United States needs to conduct its national defense strategy comes from defense contractors, many of whom rely heavily on their proprietary or trade-secret information to stay in business. They allow the U.S. government access to their proprietary information on the condition it will be protected. If, however, in compliance with DoD's new business strategy, such information is put in electronic form but then not adequately protected, an unauthorized individual, organization, or company could obtain access to another company's proprietary data.

Until recently, almost all such data was kept in stand-alone storage facilities, which made it relatively easy to set up access control procedures. However, it is much more difficult to control access to data that is available through the Internet. Therefore, implementing a new DoD business strategy for electronic access poses an increased—and increasing—risk of legal liability to the U.S. government because of inadequate protection of proprietary information.

Also, in all cases where access is limited and distribution strictly controlled, there must be a method for the U.S. government to indicate who may have access. Maintaining control of this data will require labeling. It is not possible to control access to sensitive electronically stored information unless it is labeled in

a way that can be universally recognized and understood. Most of the data described, including proprietary data, is either inadequately labeled or not labeled at all, making it impossible to determine the sensitivity of each item.[6] Providing adequate electronic labels for the voluminous proprietary data will undoubtedly be a time-consuming and costly undertaking.

To date, Congress has provided no funding to ensure proper access labeling of electronically stored proprietary information. Labeling will also be required to indicate whether the given document has been modified or destroyed. Known as "data integrity," this is one of the most important aspects of network security.[7] Engineers rely on the accuracy of technical drawings for all aspects of deploying and maintaining weapons systems for national defense. Since many people currently have access to this data and could modify it, verifying its authenticity is critical for research, development, testing, evaluation, and production results. Converting current hard-copy data into electronic images will entail the associated, and extremely difficult, requirement to label each file's (and subfile's) sensitivity level and unequivocally certify its authenticity.

There are three main concerns with electronically accessible proprietary information: legal liability, labeling and controlling the accuracy of data, and identity of users.

Electronic data is stored in and transmitted among a large number of repositories, local-area networks, and wide-area networks throughout the United States and several other countries. The objective of the new DoD business strategy initiative is to link all repositories and networks using the Internet to allow faster communication between federal agencies, military departments, and defense contractors. However, the larger the number of users and the more diverse the organizations involved, the more difficult it will be to control the accuracy of data and the identity of authorized users. It has been estimated that soon 1.5 million users will have authorized access to defense-related technical information.[8] These users will be U.S. military personnel, government employees, contractor personnel, and foreign nationals.

Defense contractors are companies of various sizes and organizational structures. Some include many divisions or subsidiaries, while others may be wholly owned, controlled, or influenced by other companies, organizations, or even countries. One division within a company may have authorized access to information for the performance of a specific contract that another division of the same company does not.

This implies that, given the large number of users and all the interconnectivity between repositories, networks, and diverse organizations, converting DoD technical data into electronic images will mean a reduction or loss of the ability

to confirm the identity, need-to-know, and authorization of each individual wishing access. Also, it will become increasingly difficult to keep proprietary information from being modified, destroyed, or exposed to other kinds of deliberate or unintended unauthorized disclosure, such as hacking.

CLASSIFIED INFORMATION

As the Department of Defense plan unfolds to include classified data among the types of information to be electronically accessible, two unanticipated problems have come to light: how to get the classified data securely to the desktop, and how to store and protect the data once it is there. Fortunately, moving classified information through the Internet via Type 1 encryption is now becoming possible, but desktop storage and user security are still concerns.[9]

Classified information in storage must be physically separated from other data to ensure its protection. All users handling classified data on the Internet must have independent classified storage and handling capabilities at their desks. Therefore, unless an alternative solution can be found, each user processing digitized classified information on the Internet will need a separate and secure personal computer, or a removable hard drive that is reasonably priced and user-friendly. All of the concerns about processing and protecting corporate proprietary information apply (with even greater stringency) to the processing and protection of classified national security information.

SOLUTION

The solution to the proprietary data problem centers on the labeling issue. Two possibilities come to mind. Congress could appropriate a large amount of money—possibly as much as several hundred million dollars—to create and administer a universally acceptable system of labels. The system would have to administer literally tens of thousands of data categories and access levels. The second solution would be to develop a machine capable of performing the same function.

In conclusion, it is imperative that these problems be resolved before the new defense business strategy is fully implemented. Sometimes the advantages of new technological developments disguise the problems they create. In this case, the problems especially concern data security as part of the overall DoD defensive information operations. For a variety of reasons, data security has, until recently, generally been overlooked as a matter of high priority in the digital world. So far, it appears the United States has been generally fortunate in protecting its data. However, if government funding is not soon forthcoming to accompany the new defense business strategy's plan for digitization and networked access to vast bodies of sensitive technical data, a dire price might be imposed on individual companies or even national security as a whole.

NOTES

1. Dept. of Defense, *Defense Reform Initiative: The Business Strategy for Defense in the 21st Century* (Washington, D.C.: 1997), p. iii.
2. Ibid.
3. Ibid., p. 7.
4. A complete list of the applicable requirements is available upon request.
5. *Bernstein v. U.S. Department of State*, 945 F. Supp 1279 (ND, CA 1996). See Navy Dept., "Naval Supply Systems Command," 4200 memo 0082.04 of 25 March 1997.
6. The author learned this while serving as the computer security project manager for a Joint Service Program Office from April 1998 to July 1999.
7. Deborah Russell and G. T. Gangemi, Sr., *Computer Security Basics* (Sebastopol, Calif.: O'Reilly and Assocs., 1992), p. 227.
8. The U.S. Navy and Marine Corps are currently building a joint internet that will accommodate approximately 500,000 users. If one multiplies that number by three to include the U.S. Army and Air Force, the result will be approximately 1.5 million.
9. Probably the best-known secure network now in use is the SIPRNET.