A recent pilot project proves it is feasible to exchange critical business transactions over the Net in a secure, reliable, and faster manner.

Internet Security

And the Case of Bank of America

Arie Segev, Jaana Porra, and Malu Roldan

Until recently, most firms trusted their critical electronic business transactions to external value-added network (VAN) providers. Today, however, the Internet is often proposed as an alternative to VANs as the transport medium based on the perceived low cost of the Internet, and the rapidly developing Internet security infrastructure (for example, encryption and public key management). In fact, these two obvious advantages may not be the most critical determinants in choosing how to perform electronic business transaction processing.

This article addresses some of the organizational and technical issues facing companies considering the Internet for critical business transactions. The case presented here shows how these organizational issues emerged in a two-year project study conducted at the Bank of America (BofA) [3–5]. The purpose of this project was to demonstrate the feasibility of exchanging secure payment transactions over the Internet with BofA's customer—the Lawrence Livermore National Laboratory (LLNL). Based on the lessons from this study, we suggest that an organization's Internet components must be an integral part of corporatewide information system security management, and may require a reorganization of the

Internet-related business units. Moreover, adopting the Internet for critical business transactions may not be as cost effective as technical comparisons with alternative transport media providers leads one to believe.

Security and Risk Management

Traditionally, interorganizational business transaction processing has not required changing the corporate management philosophy. Third-party VAN vendors, who control the transport medium and are perceived as being responsible for its security, own most interorganizational networks. When corporations consider the Internet as an alternative, they often treat this public network as a transport medium with little concern for its lack of management infrastructure. This translates into addressing Internet security by applying technical solutions at each of the endpoints of the interorganizational Internet application. Thus, Internet security remains a relatively technical, local, and distinct issue from the corporate level IS design and management. It involves applying secure software, hardware, firewalls and encryption methods at the Internet server or keeping the public system completely separate from the corporate network. As corporations are considering more strategic uses of the Internet, this viewpoint may need to be reconsidered. Because of the Internet's lack of central control, shifting the security responsibility away from the organization is not possible as it was with VANs. Moreover, adopting the Internet as a part of the corporate network infrastructure may require that Internet security be treated as a corporate-level security issue rather than a local technology issue.

Beyond a perception of low cost, Internet-based EDI/FEDI systems introduce two significant changes in the risk level of the corporate IS security. First, when replacing a VAN with a public network the corporate information system is open to external interaction. From the risk management viewpoint, sharing the Internet and transaction processing systems blurs the IS boundaries that formerly provided the basis for determining liability in disputes. In order to compensate, any Internet-based inter-organizational system must now include risk packaging and risk allocation plans and the organizational resources for implementing risk management. Secondly, the cost of processing exceptions must be recovered. If not designed in conjunction with a comprehensive management system, transaction-processing technology may provide a false sense of security and a misleading expectation for the financial benefits of adopting the Internet as a transport medium.

Corporate IS security models have historically emphasized the role of management in setting, maintaining, and implementing security policies, procedures, and standards. This has included developing contingency plans and disaster recovery procedures. It has also translated into setting up basic safeguards such as insurance, audits, system application controls, organizing for physical protection of hardware and facilities, and installing and managing adequate monitoring and controlling devices [2]. Corporate IS security management further includes the technical protection of software, information security, and the security of data, records, and forms. The more mature security standards and procedures exist in the older IS technologies. Currently, homogenous closed mainframe environments enjoy the most secure computing environment. The most underdeveloped and most often overlooked area of corporate IS security management is what Hutt et al. call "special security concerns" [2]. These are areas of information processing considered problematic because they were not originally designed to be a part of a corporatewide IS network. Such areas include PCs, LANs, and most important for our discussion—the Internet. The modern corporation's IS security management should be a comprehensive approach to corporate ISs and networks conducted at the strategic level. Yet today, the basic principles of corporate IS security management stand in stark contrast to most Internet security provisions. Although applying security software and hardware locally (for example, in a gateway or in an EDI/FEDI Internet server) is a step in the right direction, it is only a beginning of secure Internet business practices.

The following case study of BofA is used to illustrate the security and risk issues discussed here. This case is an example of how a special security concern (the Internet) can be managed for the secure exchange of business transactions. Most importantly, this case demonstrates that Internet security technology is available and applicable, but the organizational structures that surround the technology may be an equally important consideration.

Bank of America's FEDI/Internet Pilot Project

At the time of the pilot project, BofA was the second largest banking company in the U.S. with assets of more than $227 billion [6]. As a diversified, global financial services institution, BofA provides banking products and services to individuals, businesses, government agencies, and other financial institutions in the U.S., and in 36 other countries. The purpose of the BofA pilot project was to test the security, relia-

bility, and speed of exchanging business transactions (payment instructions) over the Internet under actual circumstances over an extended period of time. In 1994, BofA partnered with LLNL to begin exchanging limited financial transactions between the FEDI systems of the two organizations. This pilot project was to be a prototype for future business applications for the FEDI/Internet technology. In BofA, the project team consisted of representatives from marketing, telecommunications, IS services department, corporate security and a business unit called "Global Payment Services." On the LLNL side, the project group was composed of representatives from the Electronic Commerce Applications and Finance departments. The technical goal of the project was to integrate the existing FEDI application in the IS Services department at BofA with LLNL's comparable FEDI application. The transactions would be initialized on the corporate network, encrypted, and sent through an email gateway, a firewall, and then the Internet for channeling to the customer. The integration of the two organization's FEDI systems was to be made secure by using existing software packages wherever possible. One project objective was to keep the hardware and software costs under control by using existing equipment and borrowing technical expertise from the two-line organizations. From the financial viewpoint, the project was relatively inexpensive. Only two Sun workstations and some related software were purchased during the two years of the project's existence.

This case demonstrates that Internet security technology is available and applicable, but the organizational structures that surround the technology may be an equally important consideration.

The main addition to the existing FEDI system in both organizations was the Internet security component. After evaluating the current Internet security system packages, the project team chose a state-of-the-art solution based on Privacy Enhanced Mail (PEM) and its email extension called Multipurpose Internet Mail Extensions (MIME). Using PEM/MIME, the FEDI transmissions (batches of payment instructions) were encrypted on the server, transmitted over the Internet in encrypted form via email, and decrypted in a corresponding security server at the opposite end before being input to the organization's FEDI application. Most technical work required integrating the software and hardware of the corporate FEDI systems with the Internet.

The designing, coding, and testing of the FEDI system took most of the first half of 1995. In addition to the technical security system, the project team implemented a FEDI transmission management system. The key participants in both organizations carefully monitored transmissions. Descriptive transmission data, generated by the application, was distributed to designated employees on both sides using email. Daily and weekly logs of transmissions were emailed (and delivered as paper reports) to responsible parties for comparisons with the other party. These primary security monitors were supplemented by direct observations conducted by the teams. The implementation of this human-based security management system was distributed, like the project team, across organizations, functions, and organizational levels. Additional communications about the process was conducted by a system of reports, phone calls, faxes, and pagers. Weekly meetings (sometimes consisting of more than 20 representatives from all participating business units of both organizations) were used to track the process and to resolve recurring problems. Throughout the project, the existing security units from both organizations monitored the security of the network using confidential security monitoring and testing methods. Further, the groups managing the firewalls did their own local tests and monitoring procedures as a standard part of general network security procedures.

Actual FEDI transmissions began in the fall of 1995 and continued for two years. During this phase of the project, no security violations were reported. Although this cannot be taken as proof that no violations occurred (only violations discovered can be reported) both parties felt confident of the achieved security level. The performance of the pilot system was satisfactory. Each vendor bank received all customer payments within two days of the generation of the payment instructions. No messages were lost and no evidence of tampering with the data was discovered. The initial operational success convinced the project team of the viability of sending payment

instructions over the Internet using this PEM/MIME-based security system. The problems encountered during the initial phase of the project can be summarized as:

- 49% of the problems stemmed from systems being down or off-line.
- 24% were transaction delivery problems (duplicate, delayed or lost transactions).
- 17% were application/operating system incompatibilities.
- 5% were message delivery problems.
- 5% were decryption problems.

These error rates continually decreased as the project continued.

Based on the initial success, LLNL added new vendors to the system and increased the maximum allowable amounts for single payments. Additionally, LLNL expanded the use of the same process to provide travel and entertainment reimbursements to its employees. Finally, the pilot project conducted volume testing with dummy files of up to 1,000 payment transactions in each transmission batch. No security violations were encountered. Throughout the pilot project, the speed and reliability of the system remained high. Delays were mainly caused by the local FEDI applications, not the Internet components. Both parties were satisfied with the amount and quality of security monitoring conducted. Both BofA and LLNL agreed, however, that this intense management of each transmission was only possible because the volume of transmissions was low. Implementing an equally rigorous management system with high transmission volumes could be costly and labor intensive. Improving interorganizational coordination of the system that spans two corporate networks connected via the Internet could also eliminate some of the problems.

The two organizations concurred that in future implementations the amount and quality of human monitoring could be drastically reduced without compromising security. The project group concluded, however, that even with the intense monitoring of the pilot project, the delay in the discovery and resolution of security violations was much too long. This time delay would be an unrecoverable disaster for many retail electronic transactions. But in the commercial customer arena of the BofA pilot, even if the bank passes on a fraudulent transaction, it would likely be detected at the between-bank settlement systems. The pilot project demonstrated to both organizations the feasibility of using the Internet as a secure transport medium for business transactions. It is simple to conclude that the Internet is an alternative to an expensive VAN provider at the transport medium level. Does such a conclusion support the decision to implement an Internet-based transaction system at the corporate level? The answer may depend on other issues.

Product and Business-Driven Internet Security

If the Internet security problem is viewed as only a technical issue, then implemented solutions only solve specific tactical problems. In the PEM/MIME-based solution, the transactions were submitted on an as-needed basis between BofA and LLNL. PEM/MIME offered security by electronic signature and encryption combinations. Thus, PEM/MIME addressed the issue of securing the data between the BofA server and a corresponding server at LLNL. As with any other product, PEM/MIME could only serve as proof-of-concept in its designated security area (data security). During the two-year project, alternative products such as Templar from Premenos were introduced and considered. In all cases, the integration issues were relatively trivial and inexpensive compared with the potential organizational impact of the project.

Technical solutions such as the PEM/MIME-based system also have an impact on the organization in terms of how it deals with trust [7]. For example, PEM/MIME was originally designed to support a hierarchical model of trust based on official servers—not people. This means the user of the system must trust the technical arrangement instead of trusting appointed fellow workers. The problem with the automated trust approach is it assumed the PEM/MIME server could only be accessed from within the organization and by authorized individuals. With more than 100,000 employees distributed globally, the challenge of defining such organizational boundaries is real. To compensate for the inadequacy of the technical trust model, BofA considered an organizational authentication system of encryption key management. This is an example of how product-driven security may lead to unanticipated new organizational functions.

Another product-driven organizational impact relates to providing corporate-level IS security, which was formerly the responsibility of the IS department. Historically, this department was in charge of all software/hardware-based security solutions. Additionally, it controlled the few gateway servers providing access to the corporate network. Under those circumstances, product-based security was often adequate. In today's distributed world,

however, the power of the IS department has eroded. It has changed from the central broker of all information services to an on-demand service provider for the emancipated business units. One of the casualties of this transition has been the corporate-level IS security. Thus, from a corporate viewpoint, any business unit-driven security solution may fall short of satisfying the corporatewide security mission.

The Bigger Picture

When a corporation begins to exchange business transactions over the Internet, the Internet becomes part of the corporate computer network. With access now available not only to the trusted employees but to anyone else on the Internet, the scope of the security problem expands significantly. Today, employees are able to bypass established gateways for more convenient access with a modem and a telephone. This means that every computer is a potential gateway between corporate assets and the public. The technology-based approach to security and its protective measures (such as firewalls) do not take into account the emancipated corporate computer user—the most severe security threat. According to the American Society for Industrial Security survey, most attacks on Web servers are conducted by corporate insiders [1]. In today's computing environment corporate IS security is a corporate-level problem without corporate-level organizational support. Addressing these security issues by employing product-based technologies is only a tactical solution. Although the myriad of these products do perform useful functions at the point of implementation, collectively they do not represent a solution. A realistic security approach is more than just the assembling of technical components. At the strategic level, security is still a management function, not a technical issue.

A realistic security approach is more than just the assembling of technical components. At the strategic level, security is still a management function, not a technical issue.

One of the most important outcomes of the BofA pilot project was it prompted a corporate security reevaluation. This corporate-security management audit process began with identifying the organizational elements that create security problems in the new situation. These problems often occur between the computer system components. Such an audit targets locating and eliminating security imbalances in the corporate IS. By connecting the corporate network with the Internet, BofA exposed itself to a security imbalance at each interaction point between the private and public network. The resulting security audit highlighted this shortcoming.

During the pilot project, BofA and LLNL also experienced some unintentional security risks caused by common attitudes toward the PC as a personal productivity tool—not a component of a critical interorganizational IS. During the pilot project, a thoughtful employee repeatedly turned off one of the dedicated FEDI servers when leaving work. On one occasion, the keyboard of the FEDI dedicated PC was removed to be used as a spare part. Although events such as these seem more comical than risky, they cause unnecessary security alerts that prompt rigorous security management procedures at both ends of the transaction. As one team member acknowledged:

"We have a state-of-the-art security group in our corporation. But that is no longer what corporate IS security management is about. I cannot provide secure business transactions over the Internet if my people don't think secure. We are training all our employees to understand what bringing the Internet into the organization means. For a bank, security is not only an attitude. It is our business."

This viewpoint demonstrates that security can no longer be a sole concern of a security department, IT department, or telecommunications. With the sphere of computing expanding across all areas and levels of the enterprise, IS security touches everyone from the custodian to the Chief Executive Officer. If the solution to minimize these risks is purely technical, the resulting system may represent only a superficial solution. The key to security in these changing circumstances, as BofA discovered, lies not with technology, but with the organization itself.

Lessons Learned

Traditionally, implementing a new IS has had relatively limited impact on the organization. It is customary to expect that automating the business process results in increased efficiency and cost sav-

ings. These savings are often related to using computers instead of human labor. We suggest this BofA pilot project is an example of an IS that may not realize the expected cost efficiency. Adopting new technologies such as the Internet may require implementing people-intensive management structures at the process level. More importantly, however, we submit the BofA case is an example of new technologies causing potentially dramatic corporate-level change not directly driven by the implemented application or the immediate operational level processes, but by a corporate-level design process. In the BofA case this kind of change manifests itself in two ways. First, adopting new technologies may require pervasive changes in corporate policies, practices, and ISs. An example of this is at the BofA is the corporate-level IS security reevaluation prompted by the experiences with the pilot project. Second, exploiting new technologies may also require unconventional organizational solutions. From this viewpoint, the BofA pilot project may be viewed as a corporate-level prototyping process. In such a process, new technologies serve as a core for a business solution (in this case Internet/FEDI-based business applications). The participants in the project are borrowed from the existing organizational components for several years. After a prototyping phase (such as the BofA pilot project), the computer-supported service is separated into an independent business unit or a spin-off corporation. This corporate-level prototyping approach emphasizes the computer-based business application as being a corporate-level system with appropriate concern shown for planning, process design, and resource allocation. Rather than belonging to certain departments, or composed of decentralized autonomous computer-based systems, or having distributed management, systems such as the Internet/FEDI system span organizations and their inter- and intraorganizational networks. These corporate-level changes have potentially significant short-term cost consequences not anticipated in the original project plan.

The BofA pilot project is a record of testing security, reliability, and speed of transmitting critical business transactions over the Internet under actual circumstances over an extended time period. But it is also a real-life log of the central issues that similar user-driven projects in other organizations may face when implementing new technologies. Academically, we can argue the design of the pilot test could have been more rigorous. The transaction volumes might have been higher and security tests more systematic. We can also argue the number of security alerts could have been reduced with better management control. Taken out of context, the project seems to have gone through unnecessary turmoil due to inadequate planning. We suggest the BofA case described here is not unusual. The project started with the notion of the Internet as a transport medium. In such a case no organizational or interorganizational planning was anticipated. This error in judgement is in no way a sign of a lack of competence on BofA's part. Rather it represents a common underestimated scope of the change related to the introduction of the Internet into corporate systems.

Today, BofA has a better understanding of the scope of change associated with commerce over the Internet and a new business unit to manage the process.

At the BofA the pilot project was treated as a highly experimental project in terms of its subject matter, organization and methods. It was conducted in isolation from BofA's production systems and formal organization. Many of the security issues discussed arose because the pilot application was situated in a development environment.[1] The project in no way compromised BofA's high security and IS standards. The purpose of the project was to provide a proof-of-concept rather than a finished implementation. Thus, the system implemented in the experiment was considered disposable. No software, hardware, or organizational solutions of the project would be used in the actual implementation. The BofA pilot project ended in December 1996. The next phase began in 1997 and involved designing the production-level system based on the lessons learned from the pilot project. This environment was located in the bank's production environment and hence came under the protection of the bank's extensive security infrastructure.

The most important corporate-level impact of the

[1] A conversation with Mark Miyamoto, BofA.

project was the creation of a unit called Interactive Banking. The purpose of the new business unit is to continue to experiment with the Internet and related technologies in order to develop viable business ideas based on new technologies. The volunteers from the BofA pilot project largely formed the Interactive Banking unit. The aim was to combine relevant technology resources, marketing, product development, customer service talent, and security expertise into a single unit. Today, BofA has a better understanding of the scope of change associated with commerce over the Internet and a new business unit to manage the process. The utility of this project has been to demonstrate the need to anticipate and incorporate the cost of new business ideas, their management and the resulting organizational-level changes in business driven projects that apply new technologies such as the Internet. C

References

1. Cohen, F. Your firewall won't save you. *Forbes ASAP Supplement* (June 3, 1996).
2. Hutt, A.E., Bosworth, S., and Hoyt, D.B. *Computer Security Handbook.* (Third ed.). Wiley, NY, 1995.
3. Lawrence Livermore National Laboratory. Financial Electronic Data Interchange Pilot Project. Lawrence Livermore National Laboratory, Finance Department, UCRL-AR-124103, (May 1, 1996).
4. Segev, A., Porra, J., and Roldan, M. Internet-Based Financial EDI: The Case of Bank of America and Lawrence Livermore National Laboratory Pilot. The Fisher Center for Information Technology and Management, Institute of Management, Innovation and Organization, University of California, Berkeley, Working Paper CITM-96-WP, (Dec. 1996).
5. Segev, A, Porra, J., and Roldan, M. Internet based EDI strategy. *Dec. Supp. Syst. 21*, 3, (1997), 157–170.
6. Segev, A., Wan, D., Beam, C., Toma, B., and Weinrot, D. Internet-Based Financial EDI: A Case Study. The Fisher Center for Information Technology and Management, Institute of Management, Innovation and Organization, University of California, Berkeley, Working Paper CITM-95-WP-1006, (Aug. 1995).
7. Vacca, J. *Internet Security Secrets.* IDG Books Worldwide, Inc., Foster City, Calif., 1996.

Arie Segev (segev@haas.berkeley.edu) is a professor and director of the Fisher Center for Management and Information Technology at the Haas School of Business at the University of California, Berkeley.

Jaana Porra (jaana@uh.edu) is a visiting assistant professor at the Department of Decision and Information Sciences, College of Business Administration, University of Houston. At the time of this project she served as a research fellow at the Fisher Center for Management and Information at the University of California, Berkeley.

Malu Roldan (roldan@haas.berkeley.edu) is a research fellow at the Fisher Center of Management and Information Technology at the University of California, Berkeley.