Catalytic Impact of Information Technology on the New International Financial Architecture

JANE K. WINN*

I. Introduction

The sudden emergence of the Internet as a global network threatens to eclipse the importance of the global information infrastructure painstakingly built by financial institutions and their regulators over the past three decades. The open public nature of the Internet threatens the value of the closed proprietary networks developed by financial institutions that now face serious problems in integrating their legacy systems and new Internet systems. Information system security, once a dreary back office matter, is now central to the success of e-commerce business plans. Before financial institutions can capitalize on their expertise in information system security, they will have to overcome problems that have recently emerged in security of their existing legacy systems and translate their existing expertise into terms that are relevant to "e-business" security.

The challenges posed to regulated financial markets by the sudden democratization of the global information architecture may be offset by competitive opportunities only if regulated institutions can adapt quickly and effectively to the rigors of this new environment. Regulators will have to find a middle path between stifling regulated entities, permitting unregulated competitors to steal the show, and not maintaining the necessary prudential oversight of financial markets within which investors are exposed to rapidly rising levels of risk.

II. Changes in Information Technology

The recent acceleration in the growth of the global information economy caused by advances in information technology is challenging the ability of financial markets to adapt. The growth of global networked information systems creates threats to the safety and soundness of financial markets because information and transactions can flow more quickly and easily across borders, destabilizing markets in more than one country, and resulting in

*Jane K. Winn is Associate Professor, Southern Methodist University School of Law, in Dallas, Texas, and Co-Director of the Center for Pacific Rim Legal Studies. She can be reached at jwinn@mail.smu.edu or <http://www.smu.edu/~jwinn>.

more intense fluctuations in activity levels within each country. The rapid growth of networked information systems also creates threats to the security of financial market infrastructure if the trustworthiness of those networks is permitted to decline as their scope grows.[1]

Decades ago, the design of secure networked computer systems was almost the exclusive province of military and financial institutions. The first large-scale applications of sophisticated security technology using cryptography were developed in the military.[2] Banks followed closely behind, designing secure communications systems to confirm funds transfers and other sensitive information. Banks today remain at the forefront of developing sophisticated security systems for global electronic commerce,[3] although the playing field is already thick with potential competitors.[4]

An earlier generation of bank automation was based on the use of mainframe computers and closed networks.[5] One basic principal of computer security is that the larger the number of users a system has, the harder it will be to secure. Accordingly, it was not difficult to restrict access to the first generations of centralized, isolated mainframe computers. Subsequent generations of information technology, however, were not so closed and hierarchical. Enterprises began granting access to more employees and permitting the exchange of more data between enterprises. When these networks were based on leased lines or other closed communications networks, it was still feasible to establish and monitor security within the existing standards for adequate computer security.

Today, the Internet has brought tens of millions of individuals into a global computer network. The Internet lacks any central authority or formal governing body but rather is based on open, public standards and spontaneous decisions by millions of independent users. Until 1995, when the U.S. National Science Foundation (NSF) ceased providing backbone services, the NSF acceptable use policy applied to any traffic on the Internet that might be routed through its facilities and forbade commercial activity.[6] Thus, the use of the Internet for general commercial activities began only in 1995. By 1998, electronic commerce between businesses over the Internet amounted to $43 billion, while consumer transactions amounted to $8 billion, with some analysis predicting the volume of business-to-business Internet electronic commerce to grow to $840 billion in three years.[7]

---

1. TRUST IN CYBERSPACE (Fred B. Schneider ed., 1999).

2. For this reason, encryption is still regulated as a dual-use good in the export regulations of many countries, meaning that some restrictions apply to its export because it can be used for either civilian or military purposes. *See* STEWART A. BAKER & PAUL R. HURST, THE LIMITS OF TRUST: CRYPTOGRAPHY, GOVERNMENTS, AND ELECTRONIC COMMERCE (1998).

3. *See, e.g.*, Identrus (visited Feb. 21, 2000) <http://www.identrus.com/index.html> (providing that Identrus is a joint venture of several major multinational banks that plans to provide a range of electronic commerce risk intermediation services).

4. The American Bankers Association's press release on April 20, 1999 listed banking industry concerns with government electronic commerce security policies. ABA RELEASES BANKING INDUSTRY INFORMATION PROTECTION POLICY (last modified Apr. 20, 1999) <http://www.aba.com/aba/ABANews&Issues/PR_042099INFO.asp>.

5. *See* Jane K. Winn, *Open Systems, Free Markets, and the Regulation of Internet Commerce*, 72 TUL. L. REV. 1177, 1179 (1998), *available at* <http://www.smu.edu/~jwinn/esig.htm> (discussing how closed network electronic commerce differs from open network electronic commerce).

6. *Id.* at note 25. Public networks based on proprietary network protocols, such as America Online, Prodigy or Compuserve, did not have such restrictions but had more limited numbers of participants.

7. Janet Bush, *Online Revolution Tears Up Rulebook*, TIMES (London), Feb. 10, 1999, *available in* LEXIS, News Library, News Group File.

This global integration and mass market reach is creating a huge potential market for financial services. Some new financial service providers are developing wholly new information systems based on Internet standards and, as a result, are achieving rapid growth with low overheads. The most dramatic progress in this area has been achieved with online stock trading through discount brokerage firms. Consumer migration to Internet-based banking has been slower, and financial service providers have struggled to integrate Internet access and functionality with their existing legacy systems. This means setting up firewalls, proxy servers, virtual private networks, and possibly even a public key infrastructure.[8] Monitoring network security within a closed network is not easy, but it is not nearly as difficult as trying to manage access control and other security policies when tens of thousands of retail customers may be permitted to log in to a computer system. For example, a large number of unsophisticated users will make innocent or inadvertent attempts to exceed the limits of the access rights they have been granted. The large number of such attempts that occur unintentionally may mask attempts by sophisticated intruders to breach network security.[9]

One trend in electronic commerce applications today is the bundling of new products or services in order to enhance the value of a service. With the increasing complexity of services offered comes greater complexity in the risk management process associated with those services. In addition, advances in technology permit a greater volume and velocity of transaction processing to take place.[10] If responsibility for security for new projects that involve substantially greater risk than earlier undertakings is not clearly assigned or the implementation of security seems to undermine the chances for attaining the desired business objective, adequate security may never be put in place. For example, the design of secure applications using encryption technology can be very slow, expensive, and difficult. Because they are so complex, encryption applications are likely to contain design flaws that can only be discovered through extensive, expensive testing. Once installed, security based on encryption offers no perceptible benefits to users but often substantially degrades system performance, resulting in higher levels of user dissatisfaction with the process. Given that designing and implementing appropriate security will slow down a project, make it more expensive to operate, and reduce its appeal to users more concerned with convenience than security, no one will volunteer to take responsibility for such a thankless task unless the mandate to do so is absolutely clear from the highest levels of management.[11]

These increased risks to information system security are counterbalanced at least in part by greater economic opportunities offered by the mass market created by the vast number of Internet users. If regulated financial intermediaries do not act decisively to anticipate the needs of consumers logging onto the Internet, unregulated intermediaries will have a window of opportunity to develop competing products. Automating bank-customer relationships offer banks opportunities for reducing the cost of customer service while raising the level of customer satisfaction with the service received.[12] New technologies not based on

8. *See* BENJAMIN WRIGHT & JANE K. WINN, THE LAW OF ELECTRONIC COMMERCE § 3 (3d ed. 1998 & Supp. 1999) (discussing public key infrastructure and other security technologies).

9. Nick Lockett, *How to Secure Electronic Transactions*, INT'L FIN. L. REV., Mar. 1999, at 10.

10. Robert Simons, *How Risky Is Your Company?*, HARV. BUS. REV., May–June 1999, at 85, 90.

11. *See* TRUST IN CYBERSPACE, *supra* note 1, at 17.

12. Customer relationship management technologies are transforming marketing in many industries. *See, e.g.*, Megan Doscher, *Death of the Off-line Salesman*, WALL ST. J., June 21, 1999, at R16.

personal computers such as smart cards or smart telephones may also play a decisive role in defining the markets for financial services in the future. However, some new technologies, such as smart cards, may find more markets in developing countries than they have to date in the United States where markets for electronic financial services are often quite mature and customers may have little incentive to adopt newer technologies.[13]

III. Impact on Markets and Standards

New information technologies are rapidly unsettling well-established business models based on the services of third-party intermediaries in executing transactions. Some of the traditional intermediaries in addition to banks and brokerage firms adversely affected by new technologies firms include postal services, retailers, real estate agents, auctioneers, and travel agents. For example, the volume of airplane ticket sales purchased through independent travel agents in the United States is falling rapidly, from eighty percent in 1996 to only fifty-two percent in 1998.[14] The former customers of travel agents are empowered to locate the tickets they want themselves using such Internet services as Travelocity, the web interface for the SABRE airline computer reservation service.[15] In 1999, Internet transactions accounted for thirty to thirty-five percent of all stock trades by individuals, up from nothing at all in 1995.[16] The availability of Internet listing services is creating new challenges for real estate brokers.[17] Banks have faced challenges from disintermediation for many years, as alternatives to bank services, such as securitization of corporate debt and money market funds for individuals, eroded some of their core customer base. A rapid expansion of access to networked information systems by bank customers increases the number of bank services that may be disintermediated. Unlike some other groups facing the threat of disintermediation, however, regulated financial institutions often enjoy a legal monopoly over some core services that generally cannot be provided outside the regulated banking system.

Payment systems are a prime example of a process that cannot generally be provided outside regulated financial intermediaries. Regulated financial institutions generally enjoy a monopoly over deposit accounts and payment services related to them such as check processing. Nonbank competitors have begun to nibble away at the value of the core franchise that banks retain, however, and this process can only be expected to intensify with advances in information technology. Credit cards technically permit the cardholder to access a line of credit rather than providing a clear cash equivalent, but are now widely accepted in the United States and many other countries as a standard form of payment. Nonbank issuers are significant competitors of banks in the market for issuing credit cards.

---

13. *See* Symposium, *The Legal and Policy Framework for Global Electronic Commerce: A Progress Report Symposium Issue*, 14 BERKELEY TECH. L. J. 503, 512 (1999), *available at* <http://www.smu.edu/~jwinn/clashoftitans.htm> (discussing some of the reasons U.S. consumers have resisted adopting new electronic payments technologies).

14. *E-Commerce Soon to Show Benefits*, TORONTO STAR, Feb. 9, 1999.

15. *See Travelocity.com* (visited Feb. 26, 2000) <http://www.travelocity.com>. Expedia is a similar service offered by Microsoft. *See Expedia.com* (visited Feb. 26, 2000) <http://expedia.msn.com/daily/home/default.hts>.

16. *See, e.g.*, Charles Gasparino & Rebecca Buckman, *Horning In: Facing Internet Threat, Merrill to Offer Trading Online for Low Fees*, WALL ST. J., June 1, 1999, at A1.

17. *See, e.g.*, Motoko Rich, *Online Firms Jockey for Real Estate Listings*, WALL ST. J., Oct. 20, 1999, at B12; Joelle Tessler, *More People Turn to Web to Buy, Sell Homes*, WALL ST. J., July 8, 1999, at B9.

The same risk of partial migration of traditional banking services away from banks as the core providers is also present in Internet financial services markets. If Microsoft had succeeded in purchasing Intuit, the most popular personal financial management software program in the United States, Microsoft could easily have purchased a small bank located in some state with favorable banking laws and used that regulated entity for all its basic clearing and settlement functions. All the more complex forms of customer service that might be more profitable than simple clearing and settlement processing could have been done outside the bank in an environment controlled by Microsoft, not the bank. So, the existence of limited forms of government monopoly for certain financial services is no guarantee of profitability for any financial institution taking advantage of that monopoly.

While new information technologies permit disintermediation, they also permit reintermediation. Humans using networked information technology often need integration or sorting services to make sense of the bewildering array of goods and services now offered over the Internet. Consumers may not be able to articulate their need for someone to integrate disparate new services into a meaningful package. The enterprise that correctly identifies those hitherto unarticulated needs among individuals willing to use the Internet to find goods and services, however, can establish a profitable electronic commerce business. "Portals" are examples of integrators that are rapidly gaining popularity among Internet users today. For instance, Yahoo.com and other portals offer an array of services consumers are likely to need and permit individuals to customize the interface they find when dealing with the portal. Businesses that are able to establish relationships with portals can gain access to large numbers of potential customers, while businesses that attempt to operate in isolation from these new Internet intermediaries will need considerable name recognition to offset the appeal of portal services.

Internet bill presentment and payment is an example of a service that could be offered either by banks or by new technology companies such as those that offer portals.[18] It is unlikely that consumers or businesses will be willing to log on to many different websites to pay each of their different monthly bills online. Billers are unlikely to be successful in automating their billing processes if they rely on their customers to find the biller's website and authorize electronic payment from that location. Rather, both retail and business bill payers are likely to prefer to seek out an intermediary who can display for the payor a large number of bills and process payment instructions. This new form of intermediary could be a bank or it could be another type of intermediary who merely purchases access to an automated clearing house to provide payment functions.[19] Checks are the dominant method of bill payment in the United States today, and checking accounts are the exclusive domain of regulated financial intermediaries. If banks are going to remain the principal intermediaries between billers and payors, they will have to develop competitive bill presentment and payment services or see their check collection franchise erode while competitors offer new Internet services to take its place.

18. *See Council for Electronic Billing & Payment: Electronic Bill Presentment & Payment Business Practices* (visited Feb. 21, 2000) <http://www.nacha.org/billpay/business practices.htm> (discussing different business models for electronic bill presentment and payment services).

19. For example, TransPoint is an Internet bill presentment and payment service that is a joint venture of Microsoft, First Data Corporation and Citibank. For information about TransPoint, see TRANSPOINT (visited Feb. 27, 2000) <http://www.transpoint.com>.

Extremely sophisticated technologies offer the possibility of further disintermediating banks from their role of providing settlement for payment services. Some smart card services remain linked to customer accounts maintained at regulated financial institutions, but some do not.[20] The Mondex smart card is the most noteworthy example of a smart card that can transfer value between cards offline without relying on the clearing services of a financial intermediary. The spread of such systems raises profound challenges for financial market regulators as well as law enforcement authorities that rely on money laundering prosecutions as a chief weapon in fighting organized crime. The movement of substantial amounts of money in digital format outside regulated financial intermediaries threatens to make existing forms of financial market regulation and law enforcement activity ineffective. To date, however, the slow rate of adoption of such technologies in the marketplace and the cooperation of developers of such technologies with regulators have kept such risks under control.[21]

The rate at which new technology is being adopted varies across countries and regions. Financial markets in developed countries may already have considerable information technology infrastructure, but this may hinder the development of new technology as well as promote it. Financial institutions in the United States have huge investments in legacy systems that are very stable and inexpensive to operate now that they have been fully depreciated. The availability of these legacy systems may impede the introduction of new services. This seems to be happening in the competition between the relatively simple magnetic stripe card for accessing a bank or credit card account and smart cards, which offer the promise of a much richer interface between the user and the financial institution but which cannot be used until merchants and financial institutions are willing to make a huge new investment in technology. Smart cards are much more popular, by contrast, in some European and Asian countries and may find their greatest market in developing countries such as China that have not yet made much progress in automating financial services. An important factor contributing to the continued dependence of the U.S. payment system on checks is the large volume of fully depreciated sunk costs, including both equipment and human capital, shared by banks and their customers in the infrastructure of the check collection system. Given that the U.S. check collection system can be operated for only the tiny marginal costs of processing checks, the switching costs for U.S. consumers, business, and banks of adopting any wholly new payments technology will be enormous by comparison.

Although Internet access around the world is rapidly increasing, over fifty percent of all Internet users were still living in the United States in 1998.[22] The majority of Internet

20. In 1996, the U.S. Federal Reserve Board recommended revisions to its Regulation E governing electronic funds transfers to cover what it labeled "accountable" cards but not "unaccountable" smart cards. In response to congressional criticism, however, the Fed withdrew the proposal to regulate smart cards. *See* Electronic Funds Transfers, 61 Fed. Reg. 19,696 (1996) (to be codified at 12 C.F.R. pt. 205) (proposed May 2, 1996); *Report to the Congress on the Application of the Electronic Fund Transfer Act to Electronic Stored-Value Products* (visited Feb. 26, 2000) <http://www.bog.frb.fed.us/boarddocs/RptCongress/efta_rpt.pdf>.

21. *See* Walter A. Effross, *Piracy, Privacy and Privatization: Fictional and Legal Approaches to the Electronic Future of Cash*, 46 AM. UNIV. L. REV. 961 (1997) (for a complete discussion of these issues).

22. *Number of Internet Users Increasing: Philippine Study*, ASIA PULSE, Mar. 3, 1999, *available in* LEXIS News, Non-U.S. News. This study found that the worldwide number of households accessing the Internet at least once a week grew from 61 million in 1996 to 147 million in 1998 and was expected to grow to 320 million in 2000 and 720 million in 2005, by which time only 29 percent of Internet users would be found in the United States *Id.*

electronic commerce is also centered in the United States and is likely to continue for the near future although the European Union and many Asian countries are working to promote electronic commerce in their domestic economies. It is possible that the network architecture of electronic commerce outside the United States will be less dependent on personal computers as a platform. For example, the Global System for Mobile Communications has helped fuel the rapid expansion of mobile telephone networks throughout the European Union and regions outside the United States. In those areas, the cell phone may metamorphose into a personal information appliance that will promote the growth of electronic commerce outside personal computer networks.

Internet access may be difficult for potential users in developing countries, but the obstacles to access created by the difficulty of operating a personal computer will diminish as computing functions are transferred to more and more portable and wireless devices. As network access becomes possible through devices that are easier to use, more stable, developing countries may benefit from the opportunity to adopt the most sophisticated technology, skipping over intermediate or outmoded technologies. For example, the Grameen Bank, a community development bank in Bangladesh that emphasizes microlending programs, is distributing cell phones throughout Bangladesh to village women who sell calls on the cell phones by the minute to pay for them. Such village telephone services may soon upgrade to include Internet e-mail access, which would give villagers an inexpensive medium of communication with relatives abroad.[23] When the next generation of smart telephones becomes available, the same distribution system may promote the rapid spread of modern financial services to some of the world's poorest regions.

When global financial markets operated over the legacy systems maintained by regulated financial institutions, they posed serious threats to the stability of national financial markets. The magnitude of those threats only increases when the relatively stabilizing influences of institutional intermediaries are removed and unsophisticated individuals participate in markets through intermediaries that offer minimal content or guidance. For example, the U.S. Securities and Exchange Commission (SEC) has struggled to control a rising tide of securities fraud perpetrated over the Internet with repeated sweeps of Internet sites and a rising volume of enforcement actions.[24] The SEC is also reviewing the application of suitability requirements imposed on broker-dealers with regard to day trading activities by customers. Notwithstanding major efforts by regulators and others, the number of gullible investors has not stopped growing, creating opportunities for promoters touting worthless stocks to reap quick gains. The same kind of unsophisticated and uniformed investor who might lose money in a scam investment scheme can also destabilize larger market trends by rushing in or out of the market based on rumors or misperceptions.

Regulated financial intermediaries can only stabilize the operation of global markets if they retain a significant share of those markets. If regulated financial intermediaries are hobbled by burdensome regulations designed to protect the public when the public has few alternatives to regulated financial services organizations, they may be powerless to stop the erosion of their market share in favor of unregulated competitors whose operating costs

23. Manjeet Kripalani, *Telecommunications: Taking the Isolation out of Poverty*, Bus. Wk., May 3, 1999, at 136.

24. Information about the most recent sweep is available on the SEC's website. *See SEC Steps Up Nationwide Crackdown Against Internet Fraud, Charging 26 Companies and Individuals for Bogus Securities Offerings* (visited Feb. 27, 2000) <http://www.sec.gov/news/nets0599.htm>.

are lowered due to fewer costs of compliance with regulations. Regulators face a difficult task in deciding whether to lighten the regulatory burdens now imposed on financial institutions to permit them to compete more equally with nonbanks for a share of the Internet electronic commerce market or whether to try to regulate the new entrants to the marketplace. The current climate of deregulation in the United States and elsewhere will make it difficult to create new regulations to govern Internet commerce outside of a few fields.[25]

Regulators may have few alternatives to using the greater access provided by global networked computer systems as an important tool in working to make markets operate more efficiently and safely. The same access enjoyed by market participants will permit regulators to disseminate information that market participants need to make sensible decisions and to protect themselves. If markets do actually become more efficient, then many of the traditional bases for regulatory activity may diminish. Furthermore, as the U.S. SEC emphasizes, the Internet not only gives crooks a way to find gullible investors, it gives law enforcement authorities a way to find the crooks as well.[26]

IV. Challenges to Global Financial Markets

The global integration of information technology may be quite a novel phenomenon in some areas of economic activity, but financial market regulators have struggled for decades with the issues created by such developments. Financial markets can be thought of as the first organized, global information markets operating through networked computers. Financial market regulators may therefore find their problems intensifying but not particularly novel. This is in marked contrast with other information economy markets that now operate globally due to advances in information technology. Entertainment and publishing industries faced problems of piracy that seemed very significant before the creation of a global, mass market networked information system over which content could be reproduced virtually instantly, costlessly, and infinitely. Intellectual property rights owners are now struggling to find ways to upgrade the infrastructure of the network to support new digital rights management technologies to bring the threat of global piracy under control.[27]

Financial market regulators do face new challenges in maintaining the security of global financial networks. As cryptography has moved from the shadowy world of military and bank security, government controls over the use of cryptography have become a political issue.[28] In the United States and elsewhere, governments have tried to restrict exports of

25. Various governments and transnational organizations have stated that no new regulations should be imposed on the Internet without good cause shown. *See The Framework for Global Electronic Commerce* (visited Feb. 26, 2000) <http://www.whitehouse.gov/WH/New/Commerce/index.html>; *A European Initiative in Electronic Commerce* (visited Feb. 26, 2000) <http://www.cordis.lu/esprit/src/ecomcom.htm>; *A Borderless World: Realizing the Potential of Global Electronic Commerce* (visited Feb. 26, 2000) <http://www.ottawaoecdconference.org/english/announcements/e_actionoced.pdf>; *The WTO Declaration on Global Electronic Commerce* (visited Feb. 26, 2000) <http://www.wto.org/anniv/ecom.htm>.

26. Joseph F. Cella III & John Reed Stark, *SEC Enforcement and the Internet: Meeting the Challenge of the Next Millennium*, 52 BUS. LAW. 815 (1997).

27. It is unclear, however, whether such a policy of building rights management technologies into the architecture of the network is actually the most rational approach for rights holders to pursue. *See generally* CARL S. SHAPIRO & HAL VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 83–102 (1999).

28. *See* Jane K. Winn, *Cryptography and Electronic Commerce: Update on Recent Developments*, 2 J. INTERNET L. 10 (1999); BAKER & HURST, *supra* note 2.

powerful cryptography and to restrict mass market distribution of encryption technologies that might interfere with the ability of law enforcement to monitor communications.[29] Individuals and groups concerned with the preservation of traditional civil liberties in online environments have responded by attacking the weaker encryption products that governments are more willing to permit to be widely used. As a result, breaking the encryption technologies that form the backbone of today's financial market infrastructure has become a political cause among civil libertarians who have largely succeeded.[30] Financial institutions now face the challenge of upgrading their security infrastructure and making sure that the public believes in its continued safety.

Many financial institutions have actively pursued new information security technology for a strategic advantage in recent years. Several major international banks recently combined to form Identrus,[31] an electronic commerce trust organization designed to preserve the role of banks as the intermediaries for international trade in the global information economy. Zions Bank in Utah got permission from the Office of the Comptroller of the Currency to become a certificate authority under Utah's digital signature law.[32] Banks in the United States have also been involved in many electronic commerce pilot projects through the work of trade associations such as the Banking Industry Technology Secretariat[33] and the National Automated Clearing House Association.[34]

While some financial institutions may be able to leverage their current expertise into a strategic advantage, many financial institutions may confront difficult decisions about new technologies without any strategic vision to guide them. Financial institutions will have no choice but to upgrade their technological infrastructure in the coming years but are confronted by a competing array of putative successors to the leading products and services available today. Standard setting organizations and financial industry trade associations are struggling to develop new standards to guarantee interoperability as well as security but without any clear winners yet in many fields.[35]

Even standard setting organizations, with their greater access to technological expertise than many individual financial institutions, confront serious problems in trying to identify

29. The United States was once a leader in seeking such restrictions through the use of export regulations, but has recently retreated to a more moderate position. The encryption export regulations as revised in January 2000 are available at the website of the Bureau of Export Administration. *See The Office of Strategic Trade and Foreign Policy Controls* (visited Feb. 26, 2000) <http://www.bxa.doc.gov/Encryption/Default.htm>.

30. In January 1999, a group managed to decipher a message encrypted with a 56 bit key in 22 hours and 15 minutes. *See RSA Code-Breaking Contest Again Won by Distributed.Net and Electronic Frontier Foundation* (visited Feb. 26, 2000) <http://www.eff.org/pub/Privacy/Crypto_misc/DESCracker/HTML/19990119_des challenge3.html>. The group used a specially designed super computer and a worldwide network of nearly 10,000 personal computers on the Internet. *Id.*

31. *See generally Identrus* (visited Feb. 26, 2000) <http://www.identrus.com>.

32. *OCC Letter* (Jan. 12, 1998) <http://www.occ.treas.gov/ftp/release/98-4att.pdf>.

33. *See The Financial Services Roundtable* (visited Feb. 26, 2000) <http://www.bankersround.org> (providing information about BITS).

34. *See generally NACHA—The Electronic Payments Association* (visited Feb. 26, 2000) <http://www.nacha.org>.

35. For a list of various electronic payment standard setting initiatives, see the European Union Open Information Interchange (OII) Project Electronic Payment Mechanisms' website. *Electronic Payment Mechanisms* (visited Feb. 27, 2000) <http://www.echo.lu/oii/en/payment.html>. For a collection of web resources relating to electronic payment issues, see the American Bar Association Business Law Section Cyberspace Law Committee at the Subcommittee on Electronic Financial Services Subcommittee's website. *Home Page of the Subcommittee on Electronic Financial Services* (visited Feb. 27, 2000) <http://www.abanet.org/buslaw/efss/home.html>.

appropriate new technologies to create a secure and stable information infrastructure for financial markets. The most developed U.S. standards for information system security were developed for use by the military where cost-benefit balancing was not a major factor.[36] As a result, concepts such as "trustworthy" imply the highest feasible level of security, not the most appropriate level of security in light of financial constraints. In moving to a market-based standard for system security in which cost-benefit decisions must be made explicitly, fundamental questions about appropriate system security design have no clear answers. This leaves those making technology acquisition decisions without concrete guidance on practical questions about what models of security are appropriate for different business functions.

Financial institutions, thus, face a future of rapid technological innovation, increasing competition from less regulated competitors, increasing information system security risks, and no clear answers regarding what technological solutions are appropriate. These risks, however, are not utterly dissimilar to many of the risks financial institutions have always faced. These new risks may still be assimilable into the existing regulatory framework, such as risk-adjusted capital standards. Operations risk is an element of the risk-adjusted capital calculations, and many of the new information-economy-operations risks are substantially similar in type, if not in degree, to operations risks present in global financial markets operated using different networking technologies.[37] The existing framework of regulatory oversight of financial institutions creates an environment within which many of the currently unresolved issues may actually be addressed responsibly.

Risk from fluctuations in market interest rates or credit failures are nevertheless different than security risks in certain important respects. One important respect is the ability of those who suffer failures in information system security to suppress information about the failure. Disclosure of failures is essential to the development of more secure systems; yet any financial institution foolhardy enough to disclose publicly that failures have occurred in its system will suffer a loss of public confidence in its services. Because of the very real incentives for nondisclosure of information about known threats to information system security, the U.S. Critical Infrastrucure Project is designing a reporting system that permits the identity of the party disclosing a breach in security to be hidden while a database of known breaches is built for the benefit of those designing secure systems.[38]

Before the magnitude of the risks posed by new information technology can be adequately addressed within global financial markets, there is a need for the management of individual institutions to set priorities that reflect the importance of information system security. One of the characteristics of the information revolution is the sudden rise in prominence within organizations of business processes that were once thought of as mere plumbing. What were once thought of as "back office" operations designed to support other business activities are now tied directly to profitable activities. For example, the rise of data warehousing

36. *See* TRUST IN CYBERSPACE, *supra* note 1.

37. *See* JOSEPH J. NORTON, DEVISING INTERNATIONAL BANK SUPERVISORY STANDARDS 173–244 (1995) (discussing operations risk as one of the risk categories covered by the Basle Committee's standards for risk-adjusted capital adequacy). *See also Office of the Comptroller of the Currency*, NR 99–3 (visited Feb. 26, 2000) <http://www.occ.treas.gov/ftp/release/99-3.txt> (discussing technology risk management).

38. *See President's Commission on Critical Infrastructure Protection* (visited Feb. 27, 2000) <http://www.infosec.com/pccip/pccip2/> (providing information on the U.S. President's Commission on Critical Infrastructure Protection).

and data mining as activities designed to identify new market opportunities changes the focus in electronic commerce implementation from cost savings from increased efficiencies in back office operations to more successful marketing and customer service.[39] In the next generation of Internet electronic commerce, some of the most successful applications will be those that integrate sophisticated information technologies with old and new business models to produce new forms of interaction with customers online. Success in these arenas will require critical thought about not just the opportunities offered by new technologies but prudent management of the risks entailed by acting on those new opportunities.

V. Conclusion

Financial institutions were at the forefront in creating the global information economy as it exists today. New information technologies are creating new opportunities and new challenges for regulated financial intermediaries. Those that can adapt quickly and often to the rapidly changing environment of global electronic commerce may survive and prosper. However, many competitors from outside the traditional financial services industries are designing systems that try to eliminate or minimize the role of financial institutions. Not only must financial institutions be competitive in this very dynamic environment, they must grapple with rising uncertainty about the security of their core operations. National regulators and standard setting organizations will play an essential role in deciding who succeeds in this new environment, but they will have to struggle to strike an appropriate balance in the midst of such rapid change.

39. *See* PABLO HADJINIAN ET AL., DISCOVERING DATA MINING: FROM CONCEPT TO IMPLEMENTATION (Peter Cabena ed. 1998) (discussing data mining).