CHAPTER VII:

DIGITAL TRANSFORMATION: INFORMATION, INTERACTION, AND IDENTITY

By Patricia Buckley*

Just as the Industrial Revolution led to changes in existing laws, regulations, management practices, and patterns of social interactions, so too is the Information Age reshaping today's economic and social environment. Narrowly viewed, the Industrial Revolution resulted from manufacturers applying newly available power systems to their production processes that, in turn, enabled the emergence of mass production. This innovation increased productivity and led to the production of completely new products at relatively low costs. However, the Industrial Revolution also drove change in the economic, social, and legal landscapes: towns grew, workers began to organize and, in time, concerns about issues such as plant safety and air quality arose. Similarly, the information technology (IT) that underlies the digital revolution is creating new economic, social, and legal challenges, even as it increases productivity.

One of the most obvious shifts resulting from the digital revolution is the change in our relationship to information itself. We now expect that any information we need is easily and almost instantaneously accessible. However, that expectation is based on the assumption that information has been stored so it can be easily found and retrieved. Further, it requires that new, updated information continues to be produced and made available.

Digital capabilities are also reshaping interactions among individuals and organizations. Communication devices and channels continue to proliferate, expanding opportunities for interaction. The power inherent in new IT applications is being harnessed to improve the performance of organizations of all types by automating key interaction points. Effective management in this digital environment presents special challenges—from dealing with "interaction overload" (from unwanted telephone calls and email) to a loss of control (due to the complexity introduced by IT).

* Ms. Buckley (patricia.buckley@esa.doc.gov) is a Senior Policy Advisor in the Office of Policy Development, Office of the Chief Economist, Economics and Statistics Administration.

However, it is the issue of identity that may prove to be one of the most fundamental challenges we encounter in the shift to a digital economy. Challenges to the security of identity come in many forms. They range from identity theft to unauthorized access to a network (hacking) or a facility. One important area of IT research and development is in the evolution of reliable identity verification technologies. Such technologies are needed in both the physical and virtual worlds. Although such security tools are a necessity, they must be designed and implemented so that they do not ignite privacy concerns.

This chapter considers some of the changes and challenges posed by the shifts that have occurred in the environments surrounding information, interaction, and identity during this period of digital transformation.

Information

Improvements in technology continue to increase our ability to capture, store, manipulate, and display information. Declining costs and shrinking component size have accompanied these technological improvements. The combination of these trends has led to a sharp increase in the information component of many everyday devices—from disposable telephone cards that track message units to pocket-sized telephones that have contact databases and games. Businesses also benefit as IT enables the development of manufacturing equipment that not only produces the product, but also reports production-run quality and tracks its own maintenance schedule. Even the authors of this report have benefited from the improved functionality of our computers. Using sophisticated statistical software, we can now manipulate large datasets that, until recently, exceeded the storage capacity of most desktop computers.

The Internet has become key in information expansion, by providing a common protocol for communication among devices. Although increased information content and functionality is beneficial for any single device, when devices are joined together in a network their potential expands dramatically. Using the Internet, people can locate everything from the mundane (looking up a pasta salad recipe, checking a bank account balance, verifying the movie schedule) to the important (finding information on evacuation routes following a disaster, or deodorizing a child who mistook a skunk for her puppy). The Internet also makes available information that was formerly beyond easy reach, such as: a list of ongoing clinical trials from the National Institutes of Health, the English language version of Al Jazeera, or historical photographs of the Wright brothers. In addition to providing benefits to private individuals, the Internet has also become an integral part of the landscape in which government, business, and organizations function.

As individuals and organizations continue to weave the Internet into their activities and infrastructures, resolving issues of search, archiving, and protection of intellectual property rights is critical to realizing the full potential of this network of networks.

Search

Internet users depend on their Web browser's search engine, on navigational guides or portals (e.g., Yahoo!), or on stand-alone search engines (e.g., Google, Altavista, and NorthernLight) to

locate information. Since search engines use different algorithms—algorithms that may or may not have advertising expenditures as a variable—to locate items on the Internet, results can vary substantially. For example, Table 7.1 shows the top three results obtained when searching for the phrase "digital economy," using several search engines.

Table 7.1. Top Three Search Results for "Digital Economy"

Microsoft Explorer	Google	Altavista	Yahoo!
Information Highway Advisory Council	Department of Commerce Home Page	Walmart.com: Understanding the Digital Economy by Erik Brynjolfsson	Understanding the Digital Economy Conference
Barnes & Noble.com—Cyberbranding Hardcover	Amazon.com: Books: The Digital Economy: Promise and Peril In The ...	Wired 2.03: The Economy of Ideas	Amazon.com: Books: The Digital Economy: Promise and Peril In The ...
Information Technology for Management, Hardcover—Amazon.com	Department of Commerce Home Page	Understanding the Digital Economy	U.S. Government Electronic Commerce Policy

Source: Internet search on October 27, 2003.

Nor is any search engine capable of searching everything. Two of the most prominent limiting factors are related to language and file format. During a recent Online Information conference (December 2002, London) it was noted that "the most obvious access problem is that 'all the world's information' will be provided in documented form in most of the world's languages, and while Google and other search engines have interfaces in the major languages, the information that is retrieved will not necessarily be in the language of the interface."[1] Speakers at the conference went on to note that while there are almost 600 file formats according to one count (with at least half of these found on the Internet), search engines index only a small portion of these.[2]

ARCHIVING

Organizations charged with maintaining information collections, such as libraries, face significant opportunities and challenges in a digital environment. The opportunities arise because digital information is easy to replicate and transmit with no loss of quality, which makes sharing articles, books, movies, pictures, and audio recordings easy. The procession of improvements in information storage—from microfiche and microfilm to the Internet, CDs, and DVDs—has substantially increased the opportunities for information collection, storage, and sharing. This increase has many benefits. For example, teachers can bring historical photo-

[1] Laurel A. Clyde, "Search Engines are Improving but They Still Can't Find Everything," *Teacher Librarian*, June 2003.

[2] *Ibid.*

graphs from the Library of Congress collections directly to their classrooms, and voters can easily review statements made by candidates for office.

However, from an archiving standpoint, content created digitally is of particular concern. Some historic documents that once would have circulated on paper may now only be circulated electronically—for example, an e-mailed note to a member of the President's staff containing comments on a proposed treaty.

Solving the problems of digital archiving requires both a strategy and improved IT tools. The National Archives and Records Administration (NARA), given its mission of preserving the "essential evidence that documents the rights of American citizens, the actions of federal officials, and the national experience," faces a particular challenge with regard to the growing volume of e-mail communications. Recognizing that its "current systems for archival preservation of electronic records are limited in capability and ad hoc in nature…NARA launched the Electronic Records Archives (ERA) initiative," with the San Diego Supercomputer Center to improve its capabilities.[3]

On a broader level, the National Digital Information Infrastructure and Preservation Program charges the Library of Congress to work with NARA, the Commerce Department, the White House Office of Science and Technology Policy, the National Library of Medicine, the National Agricultural Library, the National Institute of Standards and Technology and "other federal, research and private libraries and institutions with expertise in telecommunications technology and electronic commerce policy" with developing the "protocols and strategies for the long-term preservation of such materials, including the technological infrastructure required at the Library of Congress."[4]

Archiving is not only a concern for organizations, such as the National Archives, but also for other government entities, businesses, and individuals that collect, archive, and preserve digital communications and documents. Every individual and organization that deals with information must devise a system to organize what they want to, or must, keep—whether paper, disk, or e-mail attachment. Organizing and storing information that may be needed in the future is a growing challenge.

CONTROL

It has always been difficult for creators of intellectual property to maintain control of their output and information technology has a long history of increasing that difficulty. Making copies of written text—whether the original was carved in stone or written on paper—has always been possible. However, technology continues to make it increasingly easier and cheap. The advent of the photocopier allowed any individual to make copies cheaply without regard to

[3] The National Academy of Sciences, "Building an Electronic Records Archie at the National Archives and Record Administration: Recommendations for Initial Development," 2003 Pre-publication copy—subject to further editorial correction.

[4] The Library of Congress, http://www.loc.gov/today/pr/2003/03-022.html

the wishes of the copyright owner and the spread of facsimile (fax) machines allowed for quick dissemination of written documents. Similarly, the creation of relatively low-cost audio and video recording devices presented challenges to those who owned music and film publishing rights.

Maintaining control of intellectual property became significantly more difficult in the digital environment. Not only can one create copies and disseminate them at virtually no cost, digital copies are equal in quality to the original.

The audio recording industry is one interesting example of an industry trying to find its equilibrium in the digital world. Napster challenged the recording industry's business model by enabling Internet users to bypass its distribution systems. In doing so, Napster also made it more difficult for the industry to control, and thereby profit from, its intellectual property (the rights to music owned by record companies and recording artists).

Although the recording industry succeeded in shutting down the free version of Napster in 2001, other services (ones that are more truly peer-to-peer and therefore more difficult to shut down) such as Morpheus and Kazaa have emerged. According to one estimate, Kazaa users number almost a quarter billion worldwide—triple the number of users that Napster had prior to its shutdown.[5] The ability of users of these online music-sharing services to swap music over the Internet called into question the market for shrink-wrapped compact discs, as well as the licensing arrangements between recording artists and their publishers. Response to this continued challenge has been twofold—litigation and the development of legitimate online markets, such as iTunes.

Interactions

IT is also transforming information exchange. Not only do people and devices have the opportunity to interact over a growing number of channels, the differing attributes of these channels are altering the activities in which people engage. From high-profile shifts, such as the proliferation of e-mail and e-commerce sites, to more behind-the-scenes shifts in activities, such as supply chain management, these new options are having a profound effect on the economic environment. The increased potential for interaction brings benefits, but also raises the specter of interaction overload.

Communication and Commerce

Innovations in IT have resulted in a proliferation of communication devices operating over a variety of channels. These devices and channels are more than simple substitutes for each other. Their underlying technologies give them unique attributes that are redefining the terms under which communications and commerce occur.

[5] "Music Industry's Aggressive Tactics Tune Out Fans on Net," *USA Today*, May 6, 2003.

Communications

As anyone who has recently filled out a school form can attest, the number of communications channels available to the members of an average household is large—home telephone number(s), and home e-mail address(es), work telephone number(s), work e-mail address(es), mobile telephone number(s), beeper number(s), etc.

Communication devices and channels proliferate because each device or channel has a different set of attributes. With communication using basic landline telephony, you make a call to a specific physical location, and someone at the location does (or does not) answer. Landline telephony is extremely robust (system outages are rare, and dropped calls are not a problem) and relatively cheap. With more sophisticated telephone systems, people can forward calls, identify callers, and store messages. Mobile telephones bring another dimension to telephony by associating the telephone number with an individual, not a location. Channels based on Internet technologies enable the ability to send anything that can be stored in a digital form to multiple select recipients or to post it for the world-at-large. Text messaging, whether over a telephone or a personal digital assistant, is another new communications type.[6]

The variety of interactions conducted widens considerably as individuals and organizations use these communications tools to redefine how they conduct many common activities. One attribute of some of the channels listed above is to diminish the importance of a user's location. The development of landline telephony meant that the parties to a conversation could be located at great distances from each other, but at stationary locations. Mobile telephony means that, within certain geographic limits, one need not know where a person is physically to communicate with him. E-mails are also non-location dependent because one can send and receive messages anywhere in the world to any account accessible over the Internet. Furthermore, Internet access is increasingly becoming a mobile communications channel due to the spread of broadband wireless Internet access (e.g., Wi-Fi).[7]

A barrage of unwanted messages—some legitimate marketing messages and other potentially fraudulent or dangerous—have accompanied this expansion in communications channels. Anyone with an e-mail account has experienced spam—unsolicited notifications spanning the range from sexual aids to illegal international money laundering schemes. Many individuals feel overwhelmed by the constant barrage. The volume of illegitimate messages also makes it more difficult for legitimate businesses to communicate with potential customers who would be interested in their offers. Attempts to provide appropriate remedies have had mixed success. Specific regulations are in place to protect children online, but, in general, individuals and organizations must rely on filtering protocols that are less than perfect. Efforts to reduce the number of telephone solicitations through the use of the "Do Not Call" list being administered

[6] This list of communication channels is not exhaustive, nor could any complete list be compiled because of the lines dividing the various channels are becoming increasingly blurred. Documents can be sent from a computer to a fax machine, telephone calls can be made using Internet, etc.

[7] See for example, Douglas Heingartner, "Roving the Globe, Laptops Alight on Wireless Hot Spots," *The New York Times*, June 5, 2003, p. G4.

by the Federal Trade Commission are currently under court challenge, even as anti-spam legislation was passed by Congress.

E-Commerce

A specific type of interaction that has received considerable attention over the past few years is electronic commerce—that is, buying and selling online. The evolution of online transactions has been both "less" and "more" than many analysts originally estimated. During the second quarter of 2003, the U.S. Bureau of the Census reported that retail e-commerce sales were $12.5 billion.[8] Although this represents only 1.5 percent of total retail sales—far from replacing in-store sales as some proponents promised—it does represent a 28 percent increase over the second quarter of 2002. E-commerce growth in the business-to-business space, has also fallen short of early expectations. Between 2000 and 2001 (the latest data available), manufacturing e-commerce (whether over the Internet or proprietary systems) increased from 18.0 to 18.3 percent of total shipments, and merchant wholesale e-commerce increased from 8.8 to 10.0 percent.[9]

However, if one considers only the dollar value of online transactions, the importance of e-commerce to the economy is underestimated. Even when the transaction does not take place online, the terms and conditions of the commercial interaction are altered by the availability of e-commerce options. A car buyer can go to the nearest dealership armed with detailed research obtained online. The local bookstore must now consider the pricing and service policies of online competitors.

E-BUSINESS PROCESS

The availability of IT products and services also impacts the processes that underlie the interactions. The term "e-business processes" refers to business activities that use information and communications technologies. E-commerce is a specific type of e-business process, as are human resource information systems, and enterprise resources planning systems.

One particularly interesting area of e-business applications is that of supply chain management. Use of IT products and services has enabled interactions between contract participants that closely rival (if not match) the quality of interaction that occurs within a firm. This gives businesses considerable leeway in determining which functions to conduct in-house and which to outsource.

While the ability to automate interactions has been available to large organizations for some time, the development of low cost, "off-the-shelf" tools has greatly expanded the use of e-business applications among smaller organizations. IT-driven changes in the ways that businesses are managing their supply chains has been so great that the statistical agencies have had to reexamine their data collection in a number of areas. (See Box 7.1.)

---

[8] US Department of Commerce, Bureau of the Census News Release, August 22, 2003. http://www.census.gov/mrts/www/current.html

[9] US Department of Commerce, Bureau of the Census, E-Stats, March 19, 2003. http://www.census.gov/estats.

Box 7.1. Challenges for Economic Data Collection: Changes in the Supply Chain

The supply chain is one area of business process where IT is providing the means for businesses to streamline and reduce costs. While new supply chain efficiencies benefit the companies undertaking such investments, the new business structures pose challenges for economic data collection.

Existing statistical programs classify business locations into industries based on their underlying production function—businesses doing similar activities are grouped together. This classification system assumes that manufacturers, wholesalers, retailers, and service businesses each perform a distinct set of functions that fit neatly into separate boxes.

As electronic information management changes the way businesses interact with each other, boundaries between these formerly distinct sectors are blurring. Manufacturers, wholesalers, and retailers all may be selling "services." Service firms in transportation and logistics may be leveraging their expertise to take on new functions such as inventory management, or other functions that traditionally have been associated with manufacturers and distributors.

The Bureau of the Census is taking steps to ensure that the data collected adequately reflects these changes in the economy. These steps include adding questions on the supply chain to the 2002 Economic Census survey forms for many industries, which were mailed to 5 million American business locations in December 2002. The questions asked were customized for particular industries. For example, in manufacturing, respondents were asked if various supply chain activities were performed by the individual location, by another establishment within the company, by another company, or not at all. Activities included product design and a series of activities related to order fulfillment (bundling or kitting, pick and pack, warehousing, breaking bulk, local delivery, long distance delivery, and processing of returned merchandise). Census also added several questions on inventory management practices and contract manufacturing practices.*

*Source: US Department of Commerce, Bureau of the Census.

MANAGEMENT

> "When a resource becomes essential to competition but inconsequential to strategy, the risks it creates become more important than the advantages it provides."[10]

Increasingly, IT is a prerequisite rather than an option for governments, businesses, volunteer groups, and households. Possessing information technology may not put you ahead, it may just keep you from falling behind. In such an environment, effective management of IT resources is critical.

The economic research cited earlier in this report indicated that the link between investments in IT and increased productivity at the firm level is often most apparent when IT investment is accompanied by organizational change. However, as the jumble of wires that inhabits the walls, ceiling, and floors of our homes and workspaces attests, adoption of IT in most enterprises has occurred in a piecemeal fashion that simply automated existing processes. Systems are justified and expanded on the basis of how well they address a specific existing need (e.g., human

[10] Nicholas G. Carr, "IT Doesn't Matter," Harvard Business Review, May 2003, p. 42.

resources, acquisition, production, etc.). Often, little thought is given as to whether the process itself needs to be changed or as to how these new systems will interact with existing systems. The new is simply overlaid on the old.

Enterprise Architecture

An unstructured approach to IT investment can cause management problems. The actual interactions occurring between people, processes, data, and the technology become obscured under a wild tangle. Many organizations facing this problem have turned to broad-scale approaches, such as enterprise architecture (EA), to gain an understanding of how the organization is operating and, therefore, how it can be improved. Further, since IT increases the amount of information available to every member of the organization, decision-makers in these organizations are thinking about how technology can be used to empower and enable each individual involved.

An enterprise's leaders must have an accurate understanding of how the enterprise operates to manage it effectively. As an enterprise's complexity increases, this task becomes more difficult. One technique for accomplishing this goal is to construct a systematic description of the enterprise—an enterprise architecture—that relates the outcome of the enterprise's activities to the contributions of its people, business processes, data, and technology. An EA provides the holistic, "outside looking in," view that enables decision makers to understand where incompatibilities, redundancies, and overlaps exist within the enterprise. It also provides insight into the extent to which individual activities are contributing to (or detracting from) the enterprise's mission.

An enterprise's EA typically reveals a very different organization than the enterprise's organizational chart, and it forces enterprise management to confront how it actually conducts business. When all the points of interaction are described, management then has the information needed to begin a review of the effectiveness of these interactions in supporting the mission and goals of the enterprise.

Collaborative Tools

IT offers opportunities for communities of interest to form, share information, and work toward common goals. Some of these collaborative spaces are casual, such as online chat rooms. Others are formal, such as a team working on a design project. Businesses, for example, are increasingly using collaborative software programs to facilitate group discussion and decision-making. Such software allows participants to interact in dedicated online spaces, engage in discussions, and share and track information. Collaborative software, like most IT tools, cannot create efficiency in a vacuum. Organizers and participants must establish rules for interaction (i.e., who can participate, how action items are distinguished from extended conversations, who is in charge of deleting obsolete items, etc.).

Box 7.2. E-Gov Initiatives Improving Government through IT: Geospatial One Stop

The E-Government Act of 2002, signed into law by the President on December 17, 2002, provides explicit legislative recognition of the transformative potential of IT. This Act, together with the E-Gov initiatives currently under development, are part of the Administration's effort to bring the activities of the Federal government into line with the reality of the current digital environment.

As an integral part of the President's Management Agenda, the cross-agency E-Gov initiatives will make it easier for citizens and businesses to interact with the government, save taxpayer dollars, and streamline citizen-to-government transactions. Geospatial One-Stop, one of 24 initiatives, illustrates how cross-agency teams are working to improve the efficiency and effectiveness of government IT spending. The information below as well as information on the other E-Gov initiatives can be found at www.egov.gov

> Geospatial data identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth. Although a wealth of geospatial information exists, it is often difficult to locate, access, share, and integrate in a timely and efficient manner. Myriad government organizations collect geospatial data in different formats and standards to serve specific missions. This results in wasteful spending on information assets, and impedes the ability of federal, state, and local government to perform critical intergovernmental operations, such as homeland security.
>
> The Geospatial One-Stop initiative will promote coordination and alignment of geospatial data collection and maintenance among all levels of government. Initiative goals include:
>
> - Developing a portal for seamless access to geospatial information
> - Providing standards and models for geospatial data
> - Creating an interactive index to geospatial data holdings at federal and non-federal levels
> - Encouraging greater coordination among federal, state, and local agencies about existing and planned geospatial data collections

Source: http://www.egov.gov

Identity

Ten years ago Peter Steiner succinctly captured one of the key issues in Internet interaction in a New Yorker cartoon showing one dog sitting at a computer talking to another dog with the caption "On the Internet, nobody knows you're a dog."[11] And the identity issue remains one of critical importance today. The shift online of many work and personal activities requires that users have some level of assurance about the identity of the people or businesses from whom they receive information or with whom they conduct business. Effective use of networks also requires that participants are confident that information and transactions are not altered during transmission or storage. They must also be confident that access to sensitive or proprietary information is limited to users entitled to access that information. Without adequate safeguards,

[11] *New Yorker Magazine*, July 1993.

businesses and individuals will bear the brunt of increased cost due to fraud and theft and, as a society, we will not fully realize the potential benefits of online activity.

Obviously, identity concerns exist beyond the online environment. The need to verify identity is of critical importance in many contexts. Port security requires that seafarers entering a harbor on a cargo ship are correctly identified and adequately screened. Financial market stability requires that investors are confident that their financial transactions occurred in the manner requested and that no one has tampered with their account balances. Residents living near a chemical or power plant need assurance that only actual employees can access the plant's control facilities.

Challenges to the security of identity include such disparate activities as identity theft, unauthorized access to a network (hacking), and unauthorized access to a facility. One important area of IT research and development is the development of technologies capable of verifying identity with a high degree of certainty. However, the use of such security tools can ignite privacy concerns.

SECURITY

Identity is a characteristic of an individual or enterprise. It is made up of a variety of attributes, such as name, social security number, fingerprint, or corporate logo. Both the identity owners and those who rely on the assurance of correct identity can suffer damage when identity is misappropriated or identity controls are bypassed.[12] Efforts such as e-authentication, biometrics, and firewalls can help increase security around various aspects of identity.

Identity Theft

Identity theft is a growing problem for both individuals and organizations. Over the last five years, the FTC reports that 27.3 million Americans were victims of identity theft, including 9.9 million during the last year alone. They report further that "identity theft losses to businesses and financial institutions totaled nearly $48 billion and consumer victims reported $5 billion in out-of-pocket expenses."[13] Sixty-seven percent of the identity theft victims reported that existing credit card accounts were misused and 19 percent reported illegal activity in their checking or savings accounts.[14]

There are many ways in which a criminal can gain enough personal information (credit card number, social security number, blank checks, etc.) to steal the identity of someone else. Some methods are decidedly low tech, such as dumpster diving, stealing a purse or wallet, or using phony telephone solicitations. However, hacked computers are a growing source for personal information that the thief will either use directly or sell to a third party.

---

[12] See for example, Judith S. Donath, "Identity and Deception in the Virtual Community," prepared for *Communities in Cyberspace*, P. Kollock and M. Smith, editors (final draft). http://smg.media.mit.edu./people/judith/Identity/IdentityDeception.html

[13] "FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billion in Losses for Businesses and Consumers," News Release, September 3, 2003 www.ftc.gov.

[14] *Ibid*.

It is not only individual criminals who are using the Internet to steal and sell information, there is a growing trend toward larger scale criminal organizations. Until recently, the Internet sales of stolen credit card information were primarily conducted by individuals. There was little organization or automation. However, the Honeynet Project and Alliance, which tracks certain illegal online activities, has found an increase in the degree of organization involved in the exchange of stolen credit card information. Hundreds of sellers of stolen credit card numbers might be linked over networks that provide "far greater automation of a number of illicit activities contributing to credit card fraud and identity theft, including: compromising merchant sites, validating and verifying stolen credit card information, and the sale or exchange of stolen information."[15]

Computer Crime

Identity theft is only one of a wide variety of crimes that can be committed using the Internet. According to the Department of Justice, online crimes cover the range from multimillion-dollar swindles, online auction scams, and business-opportunity frauds to piracy of software and other copyrighted material. Some progress is being made, however, in catching criminals who use the Internet. For example, under a coordinated initiative called Operation E-Con, the Justice Department recently reported the arrest of over 130 individuals and the seizure of more than $17 million.[16]

Another threat comes from those who—with or without malicious intent—illegally access computer systems. Symantec, an Internet security provider, conducts statistical analysis of current trends in cyber security threats by tracking real-time cyber attack activities detected by a sample set of more than 400 companies.[17] They categorize attacks into three groups: malicious code trends (worms and blended threat activity[18]), other cyber attack trends, and vulnerability trends. Symantec reports that "[b]ased on vulnerabilities that surfaced in 2002, a number of high-risk future threats have emerged, which attackers and malicious code writers are only beginning to leverage."[19]

---

[15] The Honeynet Project is an all volunteer organization of security professionals dedicated to researching cyber threats. See "Know Your Enemy—A Profile," Assessment Date: June 6, 2003. http://www.honeynet.org/papers/profiles/cc-fraud.pdf

[16] Operation E-Con is being coordinated by 43 United States Attorney's Offices nationwide, the Federal Bureau of Investment, the Federal Trade Commission, the Postal Inspection Service, Secret Service, and the Bureau of Immigration and Customs Enforcement, in addition to other state, local, and foreign law enforcement agencies. US Department of Justice, "Justice Department Announces Dozens of Arrests in Nationwide Internet Fraud Takedown, Operation E-Con," Press Release, May 16, 2003. http://www.justice.gov.

[17] According to Symantec, they maintain "one of the world's largest and most detailed repositories of cyber attack data … collected from thousands of firewalls and intrusion detection systems throughout the world."

[18] Symantec defines blended threats as attacks that combine the characteristics of viruses, worms, Trojan horses, and malicious code with server and Internet vulnerabilities to initiate, transmits and spread an attack. By utilizing multiple methods and techniques, blended threats often spread rapidly and cause widespread damage.

[19] Mark Higgins, Ed., "Symantec Internet Security Threat Report: Attack Trends for Q3 and Q4 2002," Volume 3, February 2003.

Authentication

One way to decrease the occurrence of identity theft and other types of computer crime is to increase the level of identity certainty—that is, better authentication. For strictly online communications or transactions, demand continues to grow for an electronic equivalent for signatures and contracts as online communications and transactions increase. For situations where an individual is physically present, biometric tools are being developed.

Even though electronic credentialing or authentication techniques continue to increase in sophistication, they must be continually improved to stay ahead of hackers. Further, establishing and maintaining authentication systems can be costly and complicated. For example, to reduce the proliferation of duplicative systems at the federal level, the Administration's E-Authentication initiative launched an interim gateway in 2002 as a pilot project to support the 24 government-wide E-Government initiatives. Although the gateway was successful in the interim phase, participants determined that this solution would not scale sufficiently for the gateway to handle the authentication of credentials for all of the federal agencies. Therefore, the Administration is shifting to the federated approach used by industry.[20]

IT is also playing a role in authenticating identity in situations where an individual is physically present—via technologies, such as biometrics. According to the International Biometric Industry Association, biometric authentication "is the automatic identification or identity verification of an individual based on physiological or behavioral characteristics. Such authentication is accomplished by using computer technology in a noninvasive way to match patterns of live individuals in real time against enrolled records. Examples of biometric-based technologies include products that recognize faces, hands, fingers, signatures, irises, voices, and fingerprints."[21]

Use of these technologies is likely to become more common. For example, as part of the effort to increase the security of U.S. borders, the Enhanced Border Security and Visa Entry Reform Act of 2002 mandates that all visas issued for entry into the United States incorporate biometrics by 2006. The Act does not specify what type of biometric should be used, but among the requirements that might be considered are whether the biometrics can be checked against criminal watch lists when the user enrolls, whether they guard against dual enrollment (i.e., maintaining multiple identities), and whether they verify identity at ports of entry.[22]

PRIVACY

Even as users demand assurance of the correct identity and security of websites they visit, most want to maintain their rights to privacy. For example, visitors to a web site that claims to be maintained by the National Institutes of Health (NIH) want safeguards in place that guarantee

[20] Jason Miller, "New Authentication Plan Takes Shape," *Government Computer News*, Nov 10, 2003 http://www.gcn.com/22-32/news/24101-1.html.

[21] http://www.idia.org/faqs.htm.

[22] Michael Geruso, "Looking Visa-Holders in the Eye," *Mechanical Engineering*, September 2002, pg. 26.

that the information provided on the site is indeed the unaltered information supplied by NIH. However, the same visitors do not necessarily want NIH to maintain a record of who they are and what pages they visited.

All federal government websites and almost all other reputable private websites will have a privacy policy statement linked to their website homepage. These statements disclose what information is captured when you visit or request a download, whether tracking agents such as cookies are used, how long data are kept, and whether information gathered is ever provided to third parties. Most sites that do maintain arrangements to sell or trade data offer the opportunity for a user to opt-out of the data sharing arrangement.

Statutory and regulatory safeguards to personal information privacy continue to be developed, though in a sector-specific manner. For example, the Federal Trade Commission (FTC), as part of its consumer protection mission, supports the privacy protections provided under several pieces of legislation. "Under the FTC Act, the Commission guards against unfairness and deception by enforcing companies' privacy promises about how they collect, use and secure consumers' personal information. Under the Gramm-Leach-Bliley Act, the Commission has implemented rules concerning financial privacy notices and the administrative, technical and physical safeguarding of personal information, and it aggressively enforces against pretexting. The Commission also protects consumer privacy under the Fair Credit Reporting Act and the Children's Online Privacy Protection Act."[23]

Similarly, the Department of Health and Human Services (HHS) is responsible for the regulation that enables the federal privacy protections for individually identifiable health information provided for under the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Under the Privacy Rule (published December 2000), covered entities had to have standards in place to protect and guard against the misuse of individually identifiable health information by April 1, 2003 (April 14, 2004 is the deadline for small health plans).[24]

Conclusion

While adjusting to the realities of the current digital environment is far from costless, recognizing where the challenges lie and addressing them directly will help smooth the transition.

[23] Federal Trade Commission, Privacy Initiatives http://www.ftc.gov/privacy/index.html

[24] Department of Health and Human Services, "General Overview of Standards for Privacy of Individually Identifiable Health Information," Revised April 3, 2003. http://www.hhs.gov/ocr/hipaa/guidelines/overview.pdf