DB2 and Privacy for Effective e-business
Brief

e-business Will Shape the Future

IBM chairman Lou Gerstner has said "Every now and then, a technology or idea comes along that is so profound, so powerful, so universal that its impact changes everything . . . Network computing will transform every institution in the world. It will create winners and losers. It will change the way we do business, the way we teach our children, communicate, and interact as individuals."

e-business is using the Web to communicate with your partners, to connect with your back-end data-systems, and to transact commerce putting the strength and reliability of traditional information technology together with the connectability of the Internet. To become an e-business, you:

- transform your core business processes
- build flexible, expandable e-business applications
- run a scalable, available, safe environment
- leverage knowledge and information you've gained through e-business systems

By using Internet technologies, you can transform key business processes by expanding both the business and the market, extending the value chain, and connecting the enterprise.

Forester Group has estimated that business-to-business e-commerce will grow from $17 billion to $327 billion in goods and services by 2002. Business Week projected that by purchasing over the Internet, General Electric will save $500 million over a three year time frame.

IBM can help you leverage the most value from e-business by helping you integrate your processes in an e-business framework. To be most effective, the framework must be built around your business strategy and make the best use of your data through knowledge management and business intelligence in the following areas:

- supply chain management
- customer relationship management
- ERP

Business Intelligence

Making the best use of your customer data through business intelligence will allow you to attract and retain your best customers with a precise portrait of who they are - their wants, their needs, their buying patterns. You will be able to analyze & interpret vast quantities of customer data - demographics, product purchase histories, cross-sales, service calls, Internet experiences, and online transactions, allowing you to turn information into insight and develop conclusive, fact-based strategies to gain a competitive edge through

- business retention
- customer service
- reduced fraud
- reduced expenses
- profitable business selection

Building Consumer Trust on a Secure Foundation

However, consumer attitude is affected by their confidence in how you will use their personal information. That means that consumer privacy *must* be a consideration in your e-business implementation. As Lou Gerstner said at the OECD Ministerial Conference on 10/8/98, "Privacy - this [issue] has been around a long time, but the implications grow exponentially in a digital economy of a billion connected users. These users - consumers in every nation - are going to embrace this electronic marketplace only to the degree that they trust its proprietors to protect their personal information: confidential medical or financial records, buying habits and life histories."

As far back as 1967, we have been aware of the need for privacy in the handling of consumer data. How is privacy defined? - "the right of individuals to determine for themselves when, how, and to what extent information about them is communicated to others" -- Alan Westin 1967

You must build trust on a secure foundation because you can have effective security without managing privacy, but you *cannot* manage privacy without good security. Organization-wide security processes and products enable information systems to address confidentiality, integrity, and availability risks. IBM has processes and offerings in place to help you address security in the following areas:

- security policy
- computer & network management
- compliance
- environmental & physical security
- business continuity planning
- personnel security
- classification & control of assets
- system development & maintenance
- system access controls

DB2 Security Features

DB2 security can be grouped in four key areas: authentication, authorization, privileges, and integrity.

Authentication is the process of authenticating a user as a user or as a member of a group. DB2 interfaces with the authentication system of the operating system the database runs under. Four ways to authenticate exist when operating in a client server environment (in e-business the client is the Web server):

1) Trusted client - telling DB2 that authentication was done and validated by the client, not a very secure way and not generally used in e-business)

2) Client encrypt - the user connects to the database specifying a userid and a password, but the password is encrypted so as not to flow openly on the network). The client (in this case the Web server) validates the authentication using operating system support.

3) Server - authentication is done using a userid and password that is optionally encrypted. In this case the operating system running DB2 does the authentication.

4) DCE - authentication is performed by an independent DCE security server, thereby allowing single signon to be shared by many databases or other DCE-compliant applications. The connection at the client is validated by the DCE server who returns a token passed to the database. The database then checks with the DCE server to validate it was a valid token. No password flows between the client and the database server. Using the industry-standard DCE authentication, DB2 user can further interface with other emerging e-business authentication methods such as the Entrust PKI (public key infrastructure) emerging standard. Most operating systems and DCE provide group support, so that the user can be authenticated as a member of a group. This way, authorization and privileges can be done at a group level.

Authorization involves which functions users are allowed to perform. Users can be authorized to perform a group of functions, ranging from system authorization, which allows all functions, to lower levels, such as the ability to execute the high speed LOAD utility.

Privileges constitute a finer level of security control, such as the ability to view a table or modify it. If a privilege is on a view, then it only applies to the subset of the table represented by this view. Combined with the USER special register, this allows the user to implement privileges at a row level in a table.

DB2 also supports the RUN privilege. In this mode, an application is bounded to the database. The user is then given the privilege of running the application. Users need not have any privileges on the underlying object that the application manipulates. They can run the application but cannot change the SQL statements of that application. This way additional security can be enforced since the user cannot issue any SQL statements other then the one in the application.

Integrity is the ability to control relationships in data. Integrity involves referential integrity, check constraint, and triggers.

Referential integrity (RI) can be used to enforce the relationship between tables. An example of RI is that an order cannot exist for a customer number if that number does not exist in the customer table. DB2 was the only database that exploited RI in the TPC-D industry standard benchmark (TPC-D is now obsolete and has been replaced by TPC-H**) .**

Check constraint is the ability to enforce some rules on a column of a table, such as 'salary cannot be > $200000'.

Triggers provide the ability to enforce rules other than RI between tables such as 'customer cannot be on a mailing list if it is flagged for mailing list exclusion in the customer table'.

The Privacy Problem

The Web has tremendous promise for business and all of society. Consumer needs can be met 24 hours a day, in the most knowledgeable way and with the most personalized service imaginable. But in this new global electronic environment, we must all act with a commitment for consumer privacy to help build the trust necessary to encourage the sharing of information for legitimate business use.

While privacy is not a new business issue, the emergence and growth of the Internet and other forms of network computing have changed the situation. Users are more concerned that personal information will be collected and misused by unknown parties. The quest to establish trust in the emerging system boils down to assuring the protection of personal privacy and data security. How well the business community is able to assure the effectiveness of privacy and security online may determine the ultimate success of electronic commerce**.**

Privacy is an essential component of building consumer loyalty, and maintaining an online consumer's loyalty is one of e-commerce's great challenges. Too many alternatives are available to an online consumer to risk having him go elsewhere because he is not confident about how his personal information will be handled. And even longtime customers will quickly go to a competitor if they feel their privacy has been violated.

What do consumers want? - They want **control** over the collection and use of their personally identifiable information. The major concern that consumers have over their loss of privacy is when companies use their information in ways that they have not approved, leading to loss of anonymity, possible identity theft, intrusion with junk mail and telemarketers, unauthorized access to their social security number, and misuse of financial information.

IBM's Answer

However, with IBM's help, you can develop good business practices to make privacy a competitive edge, not a problem. IBM can show you how to embed privacy practices in your processes and systems, create positive personalization environments for your e-business programs, and communicate your privacy message effectively to your core constituents.

IBM has offerings to help you create a privacy strategy to:

- identify existing collection, use, and disclosure practices
- evaluate practices using established principles
- identify problem areas
- perform risk analysis
- develop privacy policies that meet organizational objectives
- implement policies into processes and systems

DB2 and Privacy for Effective e-business
Brief

IBM security and privacy solutions enable you to create an e-business your customers can trust. IBM is enabling its security offerings to support key industry applications that help businesses make online transactions safer, more secure, and reliable, helping to create a trusted e-business environment. IBM has the skills and capabilities to assess, plan, design, implement, and run secure, private, and trusted environments. IBM and its partners offer the broadest range of security and privacy solutions available from any vendor in the IT industry. IBM's Security & Privacy Services organization is available worldwide to help customers solve problems using consistent and repeatable methodologies.

IBM integrates hardware, software, services, and research to deliver flexible, integrated end-to-end secure e-business solutions to help you gain business value and protect your enterprise. IBM has over 30 years experience in security with a rich reservoir of intellectual capital and over 500 practitioners worldwide dedicated to providing the best security and privacy services in the industry. IBM is the only vendor to provide end-to-end secure e-business solutions across major industry-leading platforms on a global basis. Security is built into the very fabric of the offerings that IBM develops, including directories, network & database management programs, operating systems, middleware, and hardware. IBM contributes to, follows, and encourages security and privacy standards to foster open, interoperable, and portable products and solutions.

IBM's world-renowned Research Division is the technology thought leader responsible for inventing DES, advanced cryptography research leading to such results as the world's first practical provably secure public key cryptography system, developing the world's first FIPS 140-1 Level 4 certified secure cryptographic coprocessor, and pioneering work in multiparty cryptographic protocols such as iKP which lead to the SET standard for secure credit card payments.

DB2 Privacy-Enabled Database Management System

IBM with DB2 is a leader in operational and data warehousing database management systems. IBM works closely with U.S. and international standards bodies to define additional function required by database management systems to be implemented by *all* vendors.

With DB2, you can easily implement automatic consumer notification when personal data is added or changed in the database, a consumer opt-in/opt-out mechanism, consumer verification of the accuracy of personal information and a report of all discrepancies, consumer access for updating personal information, and a tracking mechanism of all accesses and uses of personal information on all consumers. You can assure that personal information is used only for the purposes specified at the time of collection, that personal information is not sold, exchanged, or communicated externally without consumer consent, and that an audit trail is implemented to determine how all personal information is used.

Elements of Fair Information Practices

Responsible information handling relates to the way an organization collects and uses personally identifiable consumer information, which is any information relating to an identified or identifiable person.

Privacy practices concern the following principles:

- **Notice/Awareness** - the existence of systems containing personally identifiable consumer information should be publicly known along with the uses of the information.
- **Choice/Consent** - information should be used only for purposes specified at the time of collection unless the consumer opts to the use of the information in other ways. Information should not be sold, exchanged, or otherwise communicated to external users without consent of the consumer.
- **Access** - Consumers should have the right to see data about themselves and to correct any information that is not accurate, timely, relevant, or complete.
- **Enforcement/Recourse** - Mechanisms should be in place to assure compliance with policies and appropriate recourse to an injured party when policies are not followed. Dispute resolution mechanisms should be readily available and affordable.
- **Security/Information Quality & Integrity** - Companies that create, maintain, use or disseminate personally identifiable information must take reasonable measures to assure the reliability for its intended use and protect it from loss, misuse, alteration, or destruction.

Notice/Awareness

This issue involves openess. The existence of systems containing personally identifiable information about individuals should be publicly known along with the uses of that information. A lack of knowledge about who has access to personal information and how that information is used creates consumer concerns. A continuous consumer awareness process is the most effective way to optimize openness.

DB2 supports openess by enabling automatic consumer notification when personal data is added or changed through the use of DB2 insert/update triggers. Clear notice concerning the types of information being collected and the purposes for its collection and use can be given to consumers any time personal information is collected. Using the DB2 contact information table, a notice is sent via an insert trigger defined on the contact table to the consumer every time personal data is entered in the database. DB2 uses an update trigger to notify consumers when their information is changed (such as confirming a change of address or change of allowed use for the information).

Choice/Consent

This element involves limits to the collection of personal information. Information should be collected *only* with the knowledge and consent of the individual. The information should be used only for purposes specified at the time of collection unless the consumer opts to the use of the information in other ways. Personal information should not be sold, exchanged, or otherwise communicated to external users without the consent of the individual.

DB2 enables protection of information use through the DB2 AUDIT facility and DB2 Opt-In/Opt-Out tables.

The security provided by DB2 views ensures that people only have access to that information that they need to access. Further, the DB2 AUDIT facility can capture all requests done by an agent for audit purposes. The information from the DB2 audit trace can be stored in the database and queried if fraud is suspected or an individual requests how his information was used.

For certain types of personal information uses, the individual's explicit consent can be obtained through an opt-in mechanism where the individual must proactively allow the use. For other types of personal information, the individual's consent is inferred through an opt-out mechanism where the individual's non-action (not checking off the opt-out) is considered to be approval for use. In either of the above two cases, a column in the table registers if the individual opted in or out. The default value (if the user does not act) depends on the rule selected.

Access

Individuals should have the right to see data about themselves and to correct any information that is not accurate, timely, relevant, or complete. The challenge lies in determining the extent to which persons should be able to amend information as well as the type of information that can be amended or removed.

IBM's family of products to develop Internet applications allows easy access to Web data:

- WebSphere
- net.data
- net.commerce

DB2 enables verification of accuracy through DB2 views, encryption, and DB2 UDFs.

For some types of personally identifiable information, you can provide the consumer with access to his information via the Web in order to verify information accuracy and report discrepancies back to the consumer. This is done via a DB2 view, joining the information to be changed with the consumer contact information, with access limited to the consumer data only based on the id and password received from the Web site (the password may be encrypted within a secure envelope). The Web application allowing a consumer to request changes uses an additional table that contains the corrected information. The data is not directly changed in the table.

For other types of personally identifiable information, you can provide the consumer with access to the information and allow the individual with means to update, change, and correct the data. This is the same way as the above except that the information provided by the consumer is updated directly in the table. Such direct update should exclude changing userid.

Enforcement/Recourse

Companies will be held accountable for complying with their privacy policies. Mechanisms to support compliance with policies and appropriate recourse to an injured party when policies are not followed. Dispute resolution mechanisms should be readily available and affordable.

DB2 enables tracking of accesses and uses of personal information to ensure quality and integrity. Using the DB2 AUDIT facility, you can track all accesses to and uses of consumer personal information (all requests are captured and kept in the database).

Security/Information Quality & Integrity

Companies should keep only personal data relevant for the purposes for which it has been gathered, consistent with principles of awareness and choice. To the extent necessary for those purposes, the data should be accurate, complete, and current. Companies should keep a record of how personal information has been used. DB2 interfaces to HSM to allow data to be migrated to tape and recalled automatically.

IBM Privacy Consulting

IBM holds a strong conviction - backed by years of market and technology experience - that when an organization strikes the right balance between privacy expectations and its use of information, it's doing the RIGHT THING: for its customers, certainly, but also for its business success.

- IBM is the leading provider of e-business privacy consulting solutions
- Using 3 decades of security and privacy intellectual capital and industry expertise, IBM has developed an approach to help companies:
  - identify the privacy issues related to their business
  - assess their level of compliance to laws, regulations and policy
  - determine the impact to their systems and processes
  - provide an estimate of the cost of implementation of a privacy program
- In doing this we target these 5 key areas:
  - strategy planning and development
  - communication management
  - customer preference management
  - sales and service customer contact
  - business and resource operations
- IBM Global Services' privacy consulting offers:
  - privacy workshops
  - assistance in the development of implementation strategy to build customer trust and position company for increased customer satisfaction and competitive advantage

IBM Privacy Architecture

The IBM Privacy Architecture has guided IBM's strategy of providing comprehensive privacy facilities across a company's systems and processes. The IBM Privacy Architecture is based on a set of commonly accepted requirements for maintaining privacy over personally identifiable information as determined by fair information practices, which include notice, choice, access, integrity, and enforcement.

The IBM Privacy Architecture begins with a sound corporate policy that defines the company's posture with respect to privacy. The policy should define what information is collected, how the information will be used, and the choices the individual has with respect to those factors. The policy should address both the online and offline collection and use of information.

The policy should consider the legal requirements of the countries and jurisdictions where the company conducts or solicits business, and be supported by appropriate administrative procedures and well defined technical processes.

Each of these should address the basic principles of notice, choice, access, integrity, and enforcement.

The IBM Privacy Architecture requires a foundation of a well defined, enterprise-wide security architecture. This architecture should meet the minimum requirements of the IBM Security Architecture (ISO standard 7498-2). The IBM Security Architecture specifies a set of common security services that address the needs of dynamic and sensitive environments. These services are identification and authorization, access control, confidentiality, data integrity, non-repudiation, and security management, including rigorous audit requirements.

IBM Privacy Implementation Model

In October 22, 1998, IBM announced new privacy consulting services, becoming one of the first companies in the industry to help businesses understand and address the growing number of issues about protecting the privacy of personal data online. IBM's Privacy Consulting Service is designed to help create and enable effective, proactive strategies that address these and other privacy-related issues.

"Practically every company doing business on the Web today collects some kind of personal data with each transaction," said Neil Isford, vice president, e-business services, IBM Global Services. "Knowing the right way to collect, manage, and protect the privacy of this data is becoming increasingly important for all businesses -- large and small. There are very specific things businesses will need to know about how to protect the privacy of the personal data they collect and steps they will have to take to comply with a variety of industry and government guidelines. IBM's privacy consulting service is designed to help them create and enable effective, proactive strategies that address these and other privacy-related issues."

"Our focus on secure information management coupled with a commitment to privacy can lead to stronger, more beneficial relationships between companies and their employees and customers," said J.C. (Cal) Slemp III, global offering executive - security, IBM Global Services. "We believe security is an essential foundation for privacy, which in turn, enables a level of trust that will help move e-commerce forward.

July 16, 1999 IBM announced a methodology at the core of their privacy consulting services that delivers a clear plan for privacy readiness. The tool-assisted methodology shows the steps involved and the questions that need to be addressed to set up the right privacy policies and systems. "The fact that IBM has institutionalized its privacy intellectual capital into a tool means that the company can identify both the hard costs such as new systems and upgrades," said Ellen Carney, director and principal analyst, Dataquest, “but also the ‘soft’ costs that many potential customers didn't even consider.”

The two core elements of IBM's new privacy services include:

A privacy workshop, which helps decision-makers identify strategies for responsible handling of customer information. It also defines management action plans. Such strategies enable companies to provide Web-based services that meet their customers’ privacy expectations in concert with applicable laws and regulations.

Privacy strategy and implementation, which helps businesses develop and implement an effective consumer and employee privacy strategy. The resulting implementation can help define an effective privacy policy, address issues such as e-business, data warehousing and data mining, and customer relationships. An additional aspect of this service presents ways to position a company for increased customer satisfaction and competitive advantage.

IBM Security and Privacy Consulting is part of IBM's broad range of e-business security services, which help companies worldwide build and maintain secure information systems. IBM has traditionally offered its customers proven technologies and innovative widely-accepted security solutions for the rapidly changing computing environment. Today that includes providing privacy assistance to clients wishing to guard against legislative and regulatory threats and to positively differentiate their companies for market advantage. Our focus on secure information management coupled with a commitment to privacy can lead to stronger, more beneficial relationships between companies and their customers.