BUSINESS RESEARCH YEARBOOK
GLOBAL BUSINESS PERSPECTIVES

VOLUME IX, 2002

Editors:
Jerry Biberman,
University of Scranton
&
Abbass F. Alkhafaji,
Slippery Rock University

A PUBLICATION OF THE INTERNATIONAL ACADEMY OF BUSINESS DISCIPLINES
This volume contains an extensive summary of most of the papers presented during the thirteenth annual international conference of the International Academy of Business Disciplines held in Los Angeles, California April 4–7, 2002. The focus of this year’s conference is “Managing in a Global Environment.” This volume is part of the continuing efforts of IABD to make available current research findings and other contributions to practitioners and academicians.

The International Academy of Business Disciplines (IABD) was established thirteen ago as a world wide, non-profit organization, established to foster and promote education in all of the functional and support disciplines of business. The objectives of IABD are to stimulate learning and increase awareness of business problems and opportunities in the international marketplace and to bridge the gap between theory and practice. The IABD hopes to create an environment in which learning, teaching, research, and the practice of management, marketing and other functional areas of business will be advanced. The main focus is on unifying and extending knowledge in these areas to ultimately create integrating theory that spans cultural boundaries.

Membership in the IABD is open to scholars, practitioners, public policy members, and concerned citizens who are interested in advancing knowledge in the various business disciplines and related fields.

The IABD has evolved into a strong global organization during the past fourteen years, thanks to immense support provided by many dedicated individuals and institutions. The objectives and far-reaching visions of the IABD have created interest and excitement among people from all over the world.

The Academy is indebted to all those responsible for this year’s program, particularly those who served as active track chairs. Those individuals did an excellent job of coordinating the review process and organizing the sessions. Special thanks are due to Dharam S. Rana, Jackson State University, and Jamaluddin Husain, Purdue University Calumet, who are this year’s Program Co-Chairs. Thanks also to the IABD officers and Board of Directors.

Our appreciation also extends to the authors of papers presented in the conference. The high quality of papers submitted for presentation attests to the Academy’s growing reputation, and provides the means for publishing this current volume.

The editors would like to extend our personal thanks to Ronald Johnson, Dean of the School of Management, University for his support. Special acknowledgment and thanks to Theresa Sandrowicz and Stephanie Medina of the University of Scranton for their outstanding help in preparation of this volume.
9. Establishes with management and operations a mechanism to track access to protected customer and employee information, within the purview of the organization and as required by law and to allow qualified individuals to review or receive a report on such activity.

10. Consistently instills a company-wide sensitivity to privacy concerns of customers, employees, and appropriate third parties and that such respect and regard is not only the right thing to do, but also that it makes good business sense.

11. Establishes and administers a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization’s privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.

12. Ensures compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization’s workforce, extended workforce, and for all business associates, in cooperation with human resources, information security personnel, administration, and legal counsel as applicable.

13. Initiates, facilitates and promotes activities to foster information privacy awareness within the organization and related entities. Reviews all system-related information security plans throughout the organization’s network to ensure alignment between security and privacy practices, and acts as a liaison to the information systems department.

14. Works with appropriate organization personnel involved with any aspect of release of protected customer, employee, or vendor, supplier, or partner information, to ensure full coordination and cooperation under the organization’s policies and procedures and legal requirements.

15. Maintains current knowledge of applicable federal and state privacy laws and accreditation standards, and monitors advancements in information privacy technologies to ensure organizational adaptation and compliance.

16. Serves as information privacy consultant to the organization for all departments and appropriate organizational units.

17. Cooperates with the appropriate compliance personnel, other legal entities, and organization officers in any privacy reviews or investigations.

18. Acts as a robust advocate for industry self-regulation and voluntary compliance when dealing with consumer advocates, state and federal legislatures, regulatory agencies, and other governmental authorities.

19. Works with organization administration, legal counsel, and other related parties to represent the organization’s information privacy interests with external parties (state or local government bodies) who undertake to adopt or amend privacy legislation, regulation, or standard.

20. Performs related duties as required or deemed appropriate by the Chief Executive Officer to accomplish the responsibilities and functions of the position.
Ability to transport oneself to other organizational offices, conference rooms and, on occasion, to off-site meetings, conferences, workshops, seminars, etc.

**Essential job responsibilities for the CPO position**

1. Proactively assist the organization in building a) trusting relationships, b) minimizing litigation costs, and c) eliminating public relations mishaps and blunders from abuses or mistakes in privacy-related matters with respect to:
   - customers, consumers, and clients resulting in customer satisfaction that will allow the organization to retain their business and acquire new business;
   - employees resulting in increased levels of employee commitment, satisfaction, teamwork, retention, and performance;
   - vendors, suppliers, partners, and other third parties resulting in unambiguous relationships where all parties understand, accept, and comply with the organization’s stated privacy policies and practices.

2. Provides strategic development guidance and assists in the identification, implementation, and maintenance of organization information privacy policies and procedures in coordination with organization management and administration, the Privacy Advisory Committee, and legal counsel.

3. Works with organization senior management and corporate compliance officers to establish an organization-wide Privacy Advisory Committee. Serves in a leadership role for the Privacy Advisory Committee’s activities.

4. Review business deals and marketing plans put forward, and service offerings and feature enhancements to the customers, which raise privacy concerns.

5. Performs initial and periodic information privacy risk assessments and conducts related ongoing compliance monitoring activities in coordination with the organization’s other compliance and operational assessment functions. Such activities will involve documenting all of the organization’s data flows in order to learn exactly what happens to that data and who has access to it.

6. Works with legal counsel and management, key departments, and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms, and information notices and materials reflecting current organization and legal practices and requirements.

7. Oversees, directs, delivers, or ensures delivery of initial privacy training and orientation to all employees, contractors, alliances, business associates, and other appropriate third parties.

8. Participates in the development, implementation, and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements, and responsibilities are addressed.
for Social Security insurance to a lawyer (Venture Direct, 2001). In the future as you walk by a certain department store, Sears for example, you will receive a call on your cell phone from Sears notifying you of sale inside. Your cell phone is being tracked by satellite and when you get near a designated retail site marketers will program a computer to call you and inform you of a great offer. SignalSoft Corporation, based in Boulder, Colorado, is working to develop technology that allows such location-based tracking on wireless equipment (“Chief Privacy Officer,” 2000).

These new and potential threats to privacy have convinced many that there is a problem and organizations are concerned about their privacy and consider protecting it important.” More and more organizations are doing something about it including creating a new position, Chief Privacy Officer. What follows below is a hypothetical job description for such a position.

II. JOB DESCRIPTION OF CHIEF PRIVACY OFFICER

POSITION TITLE: Chief Privacy Officer (CPO)

REPORTS TO: Chief Executive Officer

STATUS: FLSA Exempt

DATE: Today

GENERAL PURPOSE: The chief privacy officer provides a competitive advantage by creating a culture of confidentiality by overseeing all activities related to the development, implementation, maintenance of, and adherence to the organization’s policies and procedures covering the privacy of, and access to, customer, employee, partner, vendor, and supplier information in compliance with federal and state privacy laws and the organization’s information privacy practices and strategies.

ESSENTIAL JOB FUNCTIONS:

* Essential abilities and physical requirements for all organizational positions
  * Ability to orally communicate effectively with others.
  * Ability to communicate effectively in writing, using the English language.
  * Ability to work cooperatively with colleagues and supervisory staffs at all levels.
  * Ability to tolerate short, intermittent, and/or prolonged periods of sitting and/or standing in performance of job duties.
  * Ability to accomplish job duties using various types of equipment/supplies to include but not limited to pens, pencils, calculators, computer keyboards, telephone, etc.
CHIEF PRIVACY OFFICER:  
DEVELOPING A CULTURE OF CONFIDENTIALITY  

C. W. Von Bergen, Southeastern Oklahoma State University  
Barlow Soper, Louisiana Tech University  
Ahmad Rashid, Southeastern Oklahoma State University  

ABSTRACT  

There has been an increasing emphasis recently regarding privacy in the workforce. To address this issue a number of organizations are considering a new position: Chief Privacy Officer. This paper presents a job description for this position and addresses the need for increased vigilance in this area.  

I.  INTRODUCTION  

In the past decade or so technology has advanced significantly in a number of areas and is changing the horizons of personal privacy so fast that we suddenly face problems not thought of only a few years ago (Fickenscher, 2000). Computerized records may list every book you borrow or buy, as Monica Lewinsky discovered in 1998. Your personal healthcare information is more easily obtained without your knowledge by physicians, hospitals, insurers, federal and state governments, and researchers—and just about anyone or anything who can come up with a well-framed and persuasive argument as to why they or it should have such access. If you offer your candid opinion about race relations or an awkward sexual anecdote over e-mail, you run the risk it will be monitored and recorded—just ask the former president of the University of Tennessee who recently resigned amid allegations of improper conduct as identified by e-mails written to an opposite sex subordinate (Hopper, 2000). If you share it online or say it in an Internet chat room, it probably will stay forever for the enjoyment of future dates, divorce lawyers, private investigators, or reporters. Giving credit card information and Social Security numbers can invite "identity thieves" to run up your bills and possibly ruin your credit for years. Workplace concerns about your quantity or quality of work, theft or misuse or company property, revealing trade secrets, unlawful drug abuse, office romance, or genetic predisposition to disease, and other factors potentially affecting your productivity and costs to the organization have increasingly led employers to use new ways to monitor and electronically observe your performance (Thibodeau, 2000).  

There are currently over 1,000 private companies compiling comprehensive databases about individual consumers, a ten-fold increase in just five years (O'Harrow, 1998). No information appears to be too personal for companies to collect and sell, and the boundaries of consent are often ill defined or non-existent. Today a New York company offers the names of high school students according to GPA, religion, ethnicity, and SAT score (Student Marketing Group, 2001), while a hospital sells the names of its patients who may be eligible
QUALIFICATIONS:
1. An advanced degree preferably in law with significant course work and/or work experience in technology.
2. Knowledge and experience in information privacy laws, access, release of information, and release control technologies.
3. Knowledge in and the ability to apply the principles of project management and change management.
4. Excellent organization, facilitation, communication, persuasion, and presentation skills.
5. Knowledge and experience in encryption technology.
6. Ability to bridge the communication gap between technologists, lawyers, policy makers, consumers, employees, and relevant third party entries such as suppliers, vendors, and partners.
7. Ability to provide direction to others; interact effectively with others; design and administer complex projects; and provide in-house training of personnel.

III. REFERENCES

Student Marketing Group, Inc. (visited July 6, 2001).
http://www.studentmarketing.net