

# **Best Practices for Privacy and Security in IT and Outsourcing: The Legal Perspective**

SPIN MEETING MAY 11, 2004

**William A. Tanenbaum**

**Chair, Technology, Intellectual Property &  
Outsourcing Group**

**Kaye Scholer LLP**

**New York Office**

**KAYE SCHOLER**

# Presentation Focus

- WHAT ARE THE RISKS FROM THE CUSTOMER'S VIEW?
- WHAT ARE THE SOLUTIONS?
- WHAT ARE THE RISKS FROM THE PROVIDER'S VIEW?
- WHAT ARE THE SOLUTIONS?
- WHAT IS THE ROLE FOR CONTRACTS, AND HOW SHOULD THEY BE COMBINED WITH TECHNICAL SOLUTIONS?
- WHAT ARE THE NEW SOURCES OF RISKS?

# New Risks

- NEW REQUIREMENTS FROM NEW LAWS
  - CALIFORNIA DATABASE BREACH NOTIFICATION LAW
  - FOREIGN LAWS EVOLVING ALSO
- OUTSOURCING TO ACHIEVE REGULATORY COMPLIANCE
- WIRELESS CONNECTIVITY
- BETTER HACKERS
  - EASTERN EUROPEAN GENIUSES
  - IDEOLOGICALLY-MOTIVATED SABOTAGE
- ALL-IN-ONE INBOXES FOR VOICEMAIL AND EMAIL
- DISGRUNTLED U.S. EMPLOYEES AND THE WAYE SCHOLER SOFTWARE POLICE

# Additional General Trends That Heighten BPO and ITO Privacy and Security Issues

- PURE ITO – MORE ACCESS TO MORE PII/PERSONAL DATA
- BPO – DELEGATION OF CUSTOMER INTERFACING TO OUTSOURCE PROVIDER AND GATHERING, STORING AND USING PII
- INCREASE CUSTOMIZATION IN BPO
- MULTIPLE VENDORS CAN INCREASE GAPS AND LEAKS
  - CUSTOMERS SHOULD TREAT VENDORS AS STOCK PORTFOLIO
- POLITICAL ENVIRONMENT – WILL OPT IN ITO OFFSHORING BE REQUIRED? KATE SCHOLER

# Trends – Continued

- REGULATED OR NON-REGULATED INDUSTRY?
  - WHAT CONSTITUTES ADEQUATE EMPLOYEE BACKGROUND CHECKS?
- DISASTER RECOVERY SITES; BUSINESS CONTINUITY PROGRAMS
  - REQUIRED BY REGULATION?
- SMALL VENDORS CAN'T AFFORD DISASTER RECOVERY SITES

# Over-the-Horizon Issues

- COMING “PATENT WARS” OVER BPO BUSINESS METHOD PATENTS
- COMING “DOMAIN/TRADEMARK WARS” WHEN DOMAIN NAMES ARE VIRTUAL PHONE NUMBERS IN A VOICE OVER IP WORLD
- IP AND NON-IP PROTECTION FOR DATA AND DATABASES
- PRIVATE INFORMATION NEEDS TO BE EXCLUDED FROM BOILERPLATE CONFIDENTIALITY AGREEMENTS
- COMBINATION OF E-SIGNATURE LAWS AND BOILER AMENDMENT PROVISIONS CAN ALLOW UNINTENDED AMENDMENT OF NEGOTIATED AGREEMENTS BY WEBSITE AND ONLINE TERMS
- HIDDEN USES OF OPEN SOURCE SOFTWARE

# What Are the Provider's Risks?

- LEGAL LIABILITY FOR BREACH OF STATUTORY OBLIGATIONS
  - U.S. LAW
  - FOREIGN LAW
- BREACH OF CONTRACTUAL OBLIGATIONS EVEN IF NO STATUTORY OBLIGATION
- LIABILITY FOR SUBCONTRACTORS' ACTIONS OR INACTIONS
- LIABILITY TO INDIVIDUAL CUSTOMER OF OUTSOURCE CUSTOMER
- RISK OF SHARED RESPONSIBILITY

# How Can Provider's Risk Arise?

- TECHNICAL FAILURE
- MANAGEMENT FAILURE
  - UNAUTHORIZED ACCESS BY EMPLOYEES
  - BREACH OF SYSTEM BY NON-EMPLOYEES
  - INTERNAL CONTROLS NOT FOLLOWED
- FOREIGN LAW ISSUES
  - SEPARATE CONSIDERATION NEEDED UNDER CHINESE LAW
- MAIN SYSTEMS ARE SECURE, BUT BACKUP PROCEDURES ALLOW UNAUTHORIZED ACCESS

# Provider's Solutions

- DISCLAIM STATUTORY RISK; AVOID STATUTORY STATUS
- MAINTAIN PRIVATE INFORMATION ON CUSTOMER'S SERVERS
- PURGE INFO FROM PROVIDER'S COMPUTERS AS SOON AS POSSIBLE
- PUT CONTROL OF PASSWORD REVOCATION WITH CUSTOMER
- CONDUCT DUE DILIGENCE OF CUSTOMER

# What Are the Risks? The Customer Perspective

- LOSS OF DATA INTEGRITY
- THEFT OF PERSONALLY IDENTIFIABLE INFORMATION, CREDIT CARD INFORMATION, SOCIAL SECURITY NUMBERS, ETC.
- UNAUTHORIZED DISCLOSURE OF INTELLECTUAL PROPERTY
- LOSS OF OTHER DATA OF CUSTOMERS OF CUSTOMER
- LOSS OF CONFIDENCE IN BUSINESS OPERATIONS OF CUSTOMER BY ITS CUSTOMERS
- LEGAL LIABILITY
- IF THE PROVIDER DOES NOT HAVE ADEQUATE

# What Are Customer's Risks? (2)

- BLACKMAIL BY PROVIDER'S EMPLOYEES
- BLACKMAIL BY PROVIDER'S SUBCONTRACTORS
- SABOTAGE OF DATA OR CODE
- RISKS OF UNAUTHORIZED DISCLOSURE CAN START AT RFP STAGE AND CONTINUE DURING VENDOR SELECTION ROUNDS

# What Are Customer's Solutions?

- NEED FOR PRE-AGREEMENT CONFIDENTIALITY AGREEMENT
- EMPLOYEE BACKGROUND CHECKS
  - WHAT IS AVAILABLE IN OFFSHORE COUNTRIES?
- WHEN BACKGROUND CHECKS ARE NOT AVAILABLE, CONDUCT APPLICATION INTERVIEWS AND PROVIDE CONTRACTUAL REMEDIES
- REQUIRE USE OF “LEAST PRIVILEGE”
- IMPOSE DUTY TO DISCLOSE ON PROVIDER
- BUT WHAT IS REQUIRED IN THE POST-9/11 REGULATORY WORLD?

# Achieving Workable Legal Specificity: Contractual Use of “Security Grid” Schedule

- SECURITY GRID IDENTIFIES WITH SPECIFICITY:
  - SECURITY/PRIVACY REQUIREMENT
  - CUSTOMER’S BUSINESS REQUIREMENT FOR ABOVE
  - CUSTOMER’S TECHNICAL SPECIFICATIONS FOR MEETING REQUIREMENT
  - TECHNOLOGY AND/OR PRACTICES PROVIDER WILL USE TO MEET CUSTOMER’S REQUIREMENT
  - IMPLEMENTATION DATES FOR ADOPTION OF TECHNOLOGY FOR EACH REQUIREMENT
  - CUSTOMER’S AUDIT RIGHTS AND REMEDIES

# Customer's Due Diligence of Provider

- REVIEW BUSINESS TEAM, INCLUDING EMPLOYEES WITH SECURITY AND PRIVACY RESPONSIBILITY
- REVIEW TECHNOLOGY USED, INCLUDING SPEED OF IMPLEMENTATION OF SECURITY UPDATES
- DETERMINE IF PROVIDER MEETS INDUSTRY-SPECIFIC SECURITY STANDARDS, E.G., ISO/IEC 17799 CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT; ISO/IEC TR 13344 GUIDELINES FOR MANAGEMENT OF IT SECURITY; U.S. DEP'T OF COMMERCE NIS SPECIAL PUBLICATION 800 SERIES; EU/U.S. DEP'T OF COMMERCE PRIVACY "SAFE HARBOR" REQUIREMENTS

# Customer Due Diligence of Provider (2)

- CUSTOMER TO CONDUCT “ETHICAL HACKING” TO TEST STRENGTH
- USE OF PRIVATE NETWORKS NOT INTERNET FOR TRANSMISSION PHYSICAL AND ELECTRONIC AUDITS (MEASURED AGAINST SECURITY GRID)
- ENCRYPTION LEVELS AND TECHNOLOGY
- FIREWALLS, ANTI-INTRUSION TECHNOLOGY
- ANTI-VIRUS TECHNOLOGY
- KNOWLEDGE OF PRIVACY AND SECURITY LAWS
- REQUIRE USE OF TWO SCREENS FOR DATA ENTRY BY OFFSHORE PROVIDER EMPLOYEES

# Customer Due Diligence of Provider (3)

- IF DEDICATED SERVERS ARE NOT USED BY PROVIDER, HOW IS SECRECY MAINTAINED?
- ARE ADEQUATE LIMITS PLACED ONSITE VISITS BY THIRD PARTIES TO PREVENT ACCESS TO CUSTOMER DATA?

# Solutions to IT Risks

- TECHNICAL SOLUTIONS
  - FIREWALLS, INTRUSION DETECTIONS, ENCRYPTION, VIRUS DETECTION, OFFSITE BACKUP
- BUSINESS OPERATIONAL SOLUTIONS
  - BACKGROUND CHECKS, POLICIES AND PROCEDURES, SEPARATION OF POWERS, AUDITS
- LEGAL SOLUTIONS
  - COMPLIANCE, CONTRACTS, INSURANCE, ENFORCEMENT AUDIT

# What Policies, Procedures and Guidelines Should Be Used?

- ACCEPTABLE ENCRYPTION
- ACCEPTABLE USE
- ANALOG/ISDN LINES
- ANTI-VIRUS TECHNOLOGY
- APPLICATION SERVICE PROVIDER
- APPLICATION SERVICE PROVIDER STANDARDS
- ACQUISITION ASSESSMENT POLICY
- AUDITS
- DATABASE CREDENTIALS CODING
- DIAL-IN/REMOTE ACCESS/VPN
- DMZ LAB SECURITY
- CELL PHONE, PAGER, PDA
- EMAIL
- EMPLOYEE CONFIDENTIALITY
- EXTRANET
- INFORMATION SENSITIVITY POLICY
- INTERNAL SECURITY
- LIMIT INTERNET USAGE
- LAPTOP SECURITY
- PASSWORD PROTECTION
- PRIVACY
- RISK ASSESSMENT
- ROUTER SECURITY
- SOFTWARE ACQUISITION/LICENSING
- SERVER SECURITY
- THIRD PARTY NETWORK CONNECTION
- WIRELESS COMMUNICATIONS

# What Policies Should Be Implemented?

- INTERNAL VS. EXTERNAL POLICIES
- WHAT RESOURCES ARE AVAILABLE?
- WHAT IS CONSIDERED ACCEPTABLE FOR APPLICABLE INDUSTRY?
- WHAT ARE THE BEST PRACTICES FOR APPLICABLE INDUSTRY?
- MEASURED AGAINST THAT IS THE COST AND SCOPE OF LIABILITY

# “Trust but Verify”

- AUDIT, AUDIT, AUDIT
- SIMPLE CHECK: CUSTOMER TO DISABLE A PART OF ITS SECURITY MOMENTARILY AND MONITOR TO SEE IF PROVIDER’S POLICIES AND SYSTEMS ARE IMPLEMENTED PROPERLY
  - HOW? UNPLUG THE IDS SENSOR AND TIME HOW LONG IT TAKES THE PROVIDER TO CALL CUSTOMER TO INFORM THAT SYSTEM IS OFF LINE
  - (DO NOT DO THIS WITH EQUIPMENT OR SERVICES THAT PROVIDE PRIMARY SECURITY)

# Encryption Best Practices

- TECHNICAL ISSUES
  - BAD ENCRYPTION CAN BE WORSE THAN NO ENCRYPTION
- BUSINESS OPERATIONS ISSUES
  - ENCRYPT WHAT NEEDS TO REMAIN PRIVATE
  - CHANGE KEYS AND PASSWORDS REGULARLY
  - USE EFFECTIVE PASSWORDS
  - CUSTOMER TO AUDIT PROVIDER FOR COMPLIANCE WITH PRIVACY AND SECURITY POLICIES
- LEGAL
  - IDENTIFY AND COMPLY WITH FOREIGN LAWS REGARDING IMPORT AND USE OF ENCRYPTION
  - USE PERSONAL INFORMATION TRANSFER AGREEMENTS (“PITA’S”)

# Victim-Symptom vs. Cause-Liability

- HOST COMPUTERS HARBORING MALICIOUS CODE, PATHWAYS OR DATA
- SOFTWARE BUGS THAT ENABLE AN INTRUDER TO ACCESS AND PERFORM UNAUTHORIZED FUNCTIONS
- INSECURE NETWORK AND HOST CONFIGURATIONS
- SECURITY LOOPHOLES/BACKDOORS WITH WEAK AUTHENTICATION
- LACK OF PROPER POLICIES, PROCEDURES AND ENFORCEMENT
- WEBSITES DEFACED
- TRANSMISSION OF UNWANTED EMAIL (SPAM)
- DENIAL OF SERVICE ATTACK
- PROPAGATION OF MALICIOUS CODE
- STORAGE OF ILLICIT TOOLS OR DATA
- SHIELDING AN INTRUDER'S TRUE LOCATION OR IDENTITY
- THEFT/DESTRUCTION OF HARDWARE, SOFTWARE OR DATA

# Conduct and Contract for Serious Planning for In-Sourcing

- USE SPECIFIC SOW FOR TRANSITION SERVICES
- MILESTONES FOR TRANSITION BACK TO CUSTOMER OR SUBSTITUTE PROVIDER
- REQUIRE PROVIDER TO COOPERATE WITH CUSTOMER'S OTHER PROVIDERS
- TRANSFER OF KNOWLEDGE BASE
- TECHNOLOGY-NEUTRAL DELIVERABLES FROM PROVIDER

# Conclusions

- ADVANCED TECHNOLOGY CAN INTRODUCE PROBLEMS THAT ARE NOT ADDRESSED BY STANDARD CONTRACTS
- COMBINE CONTRACTUAL AND TECHNICAL PROTECTION
  - ENSURE THAT CONTRACTS ARE TECHNOLOGY-ADVANCED AND LAWYERS ARE TECHNOLOGY-ENABLED
- RIGHTS WITHOUT REMEDIES ARE NOT RIGHTS
- LEGAL REMEDIES MEASURED IN GEOLOGIC TIME ARE NOT EFFECTIVE
- AUDITS CONSTITUTE PRACTICAL MONITORING AND ADVANCE NOTICE OF PROBLEM

# For electronic copy of PowerPoint --

- SEND EMAIL TO  
WTANENBAUM@KAYESCHOLER.COM  
OR HAND IN BUSINESS CARD