903 Security Concerns for Global Businesses

Cynthia A. Binns
Associate General Counsel - Corporate Affairs
ICI Paints

Daniel E. Karson
Executive Managing Director & Counsel
Kroll Associates, Inc.

Douglas B. Whiting
Assistant General Counsel
Entergy Power Group

Faculty Biographies

Cynthia A. Binns

Cynthia A. Binns is associate general counsel‹corporate affairs for ICI Paints in Cleveland. She oversees corporate governance issues and immigration matters and provides primary legal support to the international and purchasing functions of the company and to the packaging coatings division.

Prior to joining ICI Paints, Ms. Binns was a corporate attorney with Nordson Corporation, a manufacturer of industrial application equipment with world headquarters in Westlake, OH.

Ms. Binns has been an active member of the Board of ACCA's Northeast Ohio Chapter for several years. She has served as president of the Chapter and in the capacities of programming cochair and pro bono cochair. Her article entitled "An Overview of Temporary U.S. Business Visas" was published in the *ACCA Docket*. She has conducted seminars on this topic for ACCA, the Federal Bar Association, the Cleveland Bar Association, and the Cleveland Association of Paralegals. Ms. Binns has been trained in mediation techniques and volunteered her services to a nonprofit conflict resolution center for over three years.

Ms. Binns is a cum laude graduate of Baldwin-Wallace College and received her JD from the Cleveland-Marshall College of Law.

Daniel E. Karson

Daniel E. Karson is executive managing director and counsel for Kroll Associates. Mr. Karson has over 25 years experience directing investigations of business crimes and regulatory violations. He also has led litigation support efforts and conducted major asset searches. He launched Kroll's European operations, opening its office in London and serving as its first managing director. He also opened Kroll offices in Boston and Philadelphia. Mr. Karson directs major investigations of fraud, grey market diversion, litigation support cases, asset searches and due diligence. Before returning to investigations work full time, he headed Kroll's Eastern North America region, the largest of its business divisions. He served as Kroll's general counsel for 11 years.

Prior to joining Kroll Associates, Mr. Karson was general counsel and assistant commissioner of the Department of Investigation of the City of New York. He was the first director of the New York City Inspector General Program and directed investigations and determined policy for the internal investigating offices of 24 mayoral agencies. His office was responsible for investigating crime and misconduct by City employees and by persons and companies doing business with the City of New York. Previously, Mr. Karson worked as an assistant district attorney for Bronx County, where he served as chief of narcotics investigations.

Mr. Karson coauthored a chapter in The Bureau of National Affairs' *Prevention of Corporate Liability Manual*. He also authored a chapter in ACCA's *Corporate Internal Investigations*. He is a board member of ACCA's Greater New York Chapter .

Mr. Karson graduated cum laude from Ithaca College and he received a JD from the New York University School of Law.

Douglas B. Whiting

Douglas B. Whiting has practiced law as an international and transactional lawyer for 19 years. He currently serves as assistant general counsel of The Entergy Power Group based in the Houston area. He manages Entergy's legal support for non-utility power plant construction, operations, and asset management issues in North America, South America, Europe, and Asia.

For the first five years of his career, Mr. Whiting worked in-house with Southern California Edison Company and its non-utility affiliates. He was one of 12 individuals with Edison Mission Energy Company at its inception, and it is now one of the largest non-utility electric power producers in the world. After Mission Energy, he became divisional general counsel for a Helsinki-based international conglomerate, A. Ahlstrom Corporation. When his division was bought out by Foster Wheeler Corporation, he managed his division's San Diego offices until he completed their shutdown. Mr. Whiting then went into private practice in San Diego where he advised primarily Fortune-500-sized corporations on domestic corporate and transactional matters and international matters relating to the electric power industry and project finance. He also conducted in-house training seminars on international management, cultural, and monetary issues for corporations.

Mr. Whiting is also a former national chair of the ACCA’s international energy committee.

He obtained his JD and MBA from the University of Utah.

American Corporate Counsel Association
Annual Meeting
October 23, 2002

Security Concerns for Global Business

Daniel E. Karson
Executive Managing Director and Counsel
Kroll Associates

Cyntha A. Binns
Associate General Counsel – Corporate Affairs
ICI Paints

Douglas B. Whiting
Assistant General counsel
Entergy Power Group

Security is now a matter of highest priority to multi-national corporations, especially corporations with headquarters in the United States.

Prior to the attack on September 11, 2001, corporate concerns about the safety of human resources, intellectual property and property usually were correlated directly to the locations where a corporation established its operations. Threats were perceived to be greater in the developing world and in politically unstable countries.

Consequently, it was well known that the most prominent international security concerns included (and still do) kidnapping for ransom in parts of Latin America and Southeast Asia; ship hijacking in Asian waters; extortion in countries of the former Soviet Union; and terrorism and expropriation in unstable political environments.

The attack on September 11, 2002 informed us that harm to employees and corporate property could occur in any country. In the last year, as the United States government and American corporations have increased security measures, the danger of a similar large scale attack in the United States has diminished. However, potential threats to employees and offices outside the United States have increased everywhere else.

Corporate security now may be considered part of the compliance responsibilities of in-house counsel. In the event of an attack on corporate resources, it is fair to assume that victims will inquire, among other things, as to whether the corporation acted prudently and took reasonable actions to protect its employees and other assets.

More than ever, corporate counsel should play a role in evaluating their company's security policies. This presentation is intended to alert counsel to the most important of those security considerations.

Key Issues in Evaluating a Corporation's Vulnerability

The areas of key importance in evaluating risk in a foreign corporate location are:

- **Political conditions in the country where the corporation has operations.** The corporation should be fully informed on political and economic conditions. Is the country in a region of political unrest or upheaval? Are there organized, terrorist or criminal extortionate groups that operate in the country that prey on business? In some cases an extortionate group could include the government or persons associated with government officials, such as was the case in Indonesia under Suharto.
- **The local form of government.** If the country does not have a democratic form of government or its nominally democratic government is immature; if the corporation is a sole source of a critical product, the corporation may be subject to political influence and interference.
- **How the corporation is identified in the foreign country.** Is it known as an American company? Does it fly an American flag alongside the national flag? How many Americans work on site? Where do they live in-country? The degree to which the corporation is identified as American can make it and its employees vulnerable.
- **Whether the corporation's industry is a higher profile target.** What does the company manufacture? Strategic lines such as defense related products, pharmaceuticals, chemicals, power generation are examples of industries that could be targets in the United States or outside.
- **How the company tranpsports its product.** Is it overly dependent on single transportation routes or means of transportation by air, land, rail or ship that could be interrupted in a period of unrest?
- **The identity of the company's vendors and major customers.** On what vendors does the corporation rely for key supplies and on what customers for revenue? Are they the captives of a disreputable vendor or customer? Does the company have government contracts? Are those contracts with the United States government or a foreign government?
- **The corporation's business partners.** Who are the principals of the corporation's joint venture partners? Who is banking their investment? Is it a financial institution or source with which the corporation is familiar?[1]

[1] Useful reference sources include:

1. The US Department of State travel advisory can be a useful, although limited resource in assessing political conditions in a country. **travel.state.gov/warnings_list.**
2. The Treasury Department has a web site identifying known money launderers. **treas.gov/ofac**
3. Enter the term **"patterns of global terrorism"** into Google or another search engine and you will get the annual reports on global terrorism published by the State Department.
4. Consult the US Chamber of Commerce in a foreign country, the US Embassy, the FBI legate in the US Embassy, or a local law firm.

Emergency Planning/Crisis Management

If the corporation waits until a emergency occurs before formulating a company wide response it will put life and property at greater risk than necessary. A general plan of response and communication must be in place before the threat occurs.

Crisis management is the ability of a company to respond properly to events that may disrupt or endanger the safety of:

- Employees
- Physical Property
- Systems
- Intellectual Property
- Revenue

Objectives of a Crisis Management Plan

The goal of a crisis management plan is to

- Minimize loss of life, property, systems and time
- Minimize business interruptions
- Maximize response efforts
- Maximize recovery efforts

In preparing an adequate crisis management plan, the corporation must 1) identify and correct weaknesses in physical plants, 2) establish procedures for emergency management and communication, 3) understand where investigative evidence can be obtained and 4) involve different levels of the corporate population in policy formulation and crisis resolution.

Physical Security of Employees and Offices

The attack on the World Trade Center could not have been prevented by the Trade Center's owner, the Port Authority of New York and New Jersey. Likewise, a corporation can do little to prevent a massive, unconventional, externally based attack on its human resources and property.

However, just as the World Trade Center did after the 1993 terrorist bombing, a corporation can take steps to prepare for a crisis and arm itself with a plan and with information that can deter the infliction of harm.

After the bombing of the World Trade Center in 1993, the Port Authority took several measures intended to prevent a similar incident. Pedestrian and vehicular access was sharply restricted. Visitors were identified, badged and photographed before being admitted to the elevator banks. The underground garage was closed permanently to parking and deliveries. Mass egress from the buildings was facilitated by upgrading the illumination of stairways and by communicating emergency procedures to building

occupants. 98% of the occupants of the Trade Center below the level of impact survived the September 11 attack.

The major security policies to be addressed are:

- Perimeter Control – access to corporate property from the outside.
- Building Access Control – access to buildings on the corporate property, including maintenance plants and parking lots.
- Interior Access Control – access to the employee population and restricted areas within general admittance buildings, such as computer facilities, server locations, telephone facilities, science laboratories and record facilities.
- Creating information systems with dual architecture, enabling business continuation in the event of damage to a facility or evacuation.
- Hazard Site Analysis of security in buildings that utilize chemical, biological and radiological substances.
- Emergency Drills and policies regarding building evacuations
- Security for large assemblies – training programs, shareholder meetings
- Mail handling

The implementation of higher levels of security

Essential considerations include:

- Electronic Card Access/Closed Circuit TV
- Badging and card entry policies

Emergency response procedures

Crisis management plans should set forth responses at different levels of alert. They should provide for individual responses to:

- Crimes and acts of violence or other attacks on employees
- Crimes and acts of violence or other attacks on property
- Threats of violence
- The consequent effects of political conditions and general health emergencies
- Hacker attacks on information systems/Denial of service
- Natural disasters and emergencies; accidents (flood, hurricane, fire, etc.)
- Reputational crisis arising from alleged product liability (Coca Cola products in Belgium; Ford/Firestone)

A Formal Crisis Management Policy

A formal crisis management policy should be promulgated with the participation of all key elements of the corporate population. General counsel should be a part of the policy making group for compliance purposes. The policy should be made public, so that the corporate population knows:

- Who will be in charge during a emergency; reporting lines of authority
- Who will comprise the emergency management team
- Where critical information can be reported and obtained, including rumor control
- Key contact telephone numbers and web sites
- Emergency evacuation, escape and rescue policies
- Defined levels of emergency conditions – identifying different kinds of emergencies and different levels of response (e.g. at what point law enforcement will be notified; at what point buildings will be evacuated)

The policy can be publicized to the employee population while at the same time preserving the confidentiality of security information such as:

- access codes to secure sites
- the locations of keys to buildings and facilities
- private contact telephone numbers to emergency managers

Corporations should field test their crisis management plans, especially the communications protocols.

Pre-employment investigations

Lying about one's background is pervasive and present at every level of job category. Pre-employment investigations are an indispensable element of enhancing security. A background investigation on a prospective employee serves two major purposes: verifying the information supplied by the applicant, and uncovering information that would disqualify the applicant from employment.

A background investigation policy at a minimum should require research on:

- Criminal history
- Civil litigation
- Judgments and liens
- Regulatory violations
- Bankruptcy
- Verification of prior employment, title, salary and length of employment

The ability one has to misrepresent a background outside the United States is even greater. Unfortunately, with the exception of the United Kingdom and certain of the current and former British Commonwealth nations, most of the public records in the United States that are available to verify claims in a resume are scarce or non-existent elsewhere.

Vendor and Customer Integrity

In foreign office locations, corporations purchase products and services from indigenous vendors. Legal services, office supplies and raw materials are just some of the kinds of purchases made from local companies. Likewise, corporations maximize opportunities to sell to foreign markets.

Many companies now carry out background investigations of their vendors. Companies, particularly those dealing in strategic materials also investigate prospective customers. They do this to assure themselves that a reasonable inquiry does not disclose affiliations with criminal elements or organizations of questionable integrity, or worse, known terrorists.

Prior to the Gulf War in 1989, the government of Iraq owned undisclosed interests in companies in the US, the UK and France in trade, engineering, software, publishing, and electronics, just to name a few.

Prominent multi-national corporations risk their reputation if they are found to have purchased from or sold to individuals or businesses with such associations. The Patriot Act and other statutes apply principally to the customers of financial institutions as they relate to "Know Your Customer" guidelines. However, many companies now undertake some form of due diligence on vendors and customers. (In most cases the cost of vendor background checks is borne by the vendor, as a condition of doing business with the company.) It is essential to identity the true principals of a company.

The Retrieval and Preservation of Evidence

General Counsel should be aware of and have available the investigative tools made available by the computerization of business systems. Whether counsel chooses to use those tools requires a judgment in each individual situation.

Technology has transformed the art of investigation and the process of gathering evidence. Almost all litigation now involves some form of evidence retrieved from electronic sources. The application of computer forensic technology can be used, among other things to retrieve evidence of crimes committed against the corporation. It can be instrumental in identifying employees threatening the security of the company.

Characters and images processed on a hard drive or diskette may be deleted from directories but are difficult to erase. Documents created in Word files and email by conspirators, stalkers, bombers, extortionists and spies, among others, have been revived by computer forensic technicians and used as evidence.

Similarly almost all the telephone numbers we enter into land lines from our offices are recorded on site by our employers. If we are provided a cell phone by our employer, the records of our telephone calls are our employer's property.

The places where electronic evidence can be located include:

- Computer hard drives
- Diskettes
- Email
- Telephone records of numbers dialed from land lines and cellular phones
- Card reader access records

The places where other documentary evidence can be located include:

- Telephone message logs
- US Mail and Express Mail waybills
- Cancelled payroll and expense checks
- Office files

Conclusion

A modern security plan for a corporation with foreign offices requires the creation and communication of a Crisis Management/Emergency Response plan. General counsel should play a leading role in identifying the corporation's crisis vulnerabilities and in creating a plan.

Companies should carry out pre-employment background investigations at all levels in all office locations. Companies should consider strongly undertaking vendor and customer integrity programs, especially if they are prominently known international companies or sell products that can be used to support an organization whose interests are inimical to the United States.

General counsel should become familiar with the kinds of information that can be retrieved as evidence within management systems, such as data stored on hard drives and email.

APPENDIX A

KROLL, INC.
Advice for Building Owners and Operators with Underground Parking Facilities

Daniel E. Karson
Executive Managing Director and Counsel

Companies can enhance garage security in varying degrees. Factors that affect corporate security strategy include:

1. The location of the building
   a. metropolitan center
   b. corporate park
   c. stand-alone facility

2. Current access to the garage
   a. access by one tenant
   b. shared access by more than one tenant
   c. use of dedicated visitor space
   d. availability of public and/or metered spaces

3. The deployment of garage attendants
   a. full time or part time
   b. attendants posted at entrances
   c. attendants posted in interior
   d. attendants posted at entrances and interior

4. The presence of a loading dock
   a. access to the loading dock
   b. dimensions of the entrance

5. Hours of operation
   a. 24/7
   b. open during specified hours
   c. card access during off hours

6. Garage design
   a. single entrance and exit v. multiple entrances and exits
   b. entrance heights and widths
   c. accessibility to the interior through dedicated exits
   d. pedestrian access to the interior from the building or the street
   e. security features of portals (rolling door closure or gate, horizontal elevator bar, etc.)

Recommendations for security enhancement under all circumstances:

1. Assign attendants to all entrances
2. Ascertain that access cannot be obtained via dedicated exits
3. Inspect all vehicles and vehicle trunks before permitting entrance. Attendants should be trained in vehicle inspection
4. Eliminate card access at times when the garage is not attended
5. Install height barriers at entrances to prevent truck entry
6. Restrict loading dock deliveries to pre-arranged appointments
7. Building Safety
   a. Make sure all building safety guideline and evacuation procedures are current and relevant to the building's present interior and exterior space design
   b. Make sure all building occupants are informed of safety guidelines and evacuation procedures

Additional recommendations for security enhancement in high security situations

1. Station attendants and inspection stations outside of and away from the garage entrance, if possible
2. Install spike strip barrier or vertically controlled entrance ramp
3. Deploy concrete stanchions around the perimeter of the office building
4. Consider closing the garage for a definite or indefinite period of time
5. Consider closing the garage to visitor and public parking

APPENDIX B

Kroll, Inc.
Matrix for Levels of Crisis Response

Threat Level	Condition	Response
One	No identifiable local or regional threat	Maintain standard security and access levels
Two	General regional threat established by state or federal authorities	Vehicle and visitor searches
Three	Specific threat to one or more campus locations	Enhance security presence and personal searches.
Four	Direct threat to targeted locations	Follow emergency/crisis management plan for the building; close doors; deny access; police presence to prevent entry

APPENDIX C

MAIL HANDLING PROCEDURES

Mail handling procedures, formerly a mundane issue, now stand with all other major corporate security concerns, as a result of the events that took place on 9-11 and the subsequent anthrax deaths. The consequences of not having adequate procedures in place can mean the difference between life and death.

This article highlights some of the major areas of concern when handling mail and related packages. It is a reminder of the precautionary measures that should be in place in our companies to ensure the safety of our employees and our facilities. Furthermore, secure handling of mail and packages must also take into account internal issues, such as the integrity of the employees who manage and who work in mailroom facilities.

Preventative Measures: Gleaned from conversations with other in-house counsel or facilities personnel and from some of the government web sites referred to at the conclusion of this article, the following is a composite sketch of recommended practices when implementing safe and secure mail handling procedures.

Ultimately, each company must view this topic from a risk analysis viewpoint. Large corporations may find that more detailed procedures should be initiated. Smaller companies may believe the recommendations can be scaled back. All facets must be considered, including management of the function, management of personnel, management of the facility itself, and management of the practices and procedures that are used.

- Management of the function
    - Appoint a manager to be responsible and accountable for mailroom security. The manager should be supported by a subordinate/ alternate for emergency response planning purposes.
    - The corporate emergency response team should periodically review and assess the procedures associated with the safe handling of mail and other incoming packages (this also could be carried out by a facilities management team; a loss prevention department; a health, safety and environmental group; etc.).
    - Ensure that procedures are in place, that the procedures are communicated to employees and that employees receive proper training.

- Management of personnel
    - Conduct pre-employment background checks of potential mailroom personnel. If the mailroom operation is sub-contracted, require that the sub-contractor conduct checks of employees assigned to your company.
    - Obtain recommendations from employees who have a direct involvement in the mailroom function as to “best practices.”

  - Train and retrain personnel in the safe and efficient handling of mail and other packages (training can be internal or external, such as seminars offered by the U.S. Postal Service); train those outside the function when it makes sense to do so (e.g., receptionist, secretary, etc., as it is not always mailroom personnel who physically receive, handle or open mail).

- Management of the facility itself (physical environment)
  - Evaluate the physical location of the facility as compared to other departments and personnel. Is the facility sufficiently isolated in the event of a mishap or some type of crisis?
  - Assess mailroom ventilation (air intake/circulation system) to determine whether it is separate and apart from other personnel or departments, and, if not, whether it should be (consider installing shut-off valves to prevent the spread of any airborne contaminants) Environmental service companies can conduct a risk assessment.
  - Maintain a secure mailroom facility (e.g., limit access; lock doors to prevent access when personnel not present, etc.)

- Management of practices and procedures
  - Assess both incoming and outgoing mail practices and procedures.
  - Assess housekeeping practices (in terms of the equipment used as well as the practices actually followed by employees, e.g. wearing of gloves, cleanliness issues, etc.).
  - Determine whether personal protective equipment, such as gloves, are readily available to protect mailroom employees.
  - Change or revise practices and procedures as needed.
  - Post details on how to handle suspicious mail (obtain posters or signs from U.S. Postal Service, for example). Assure that postings are current.
  - Solicit the thoughts and concerns of mailroom personnel and incorporate their suggestions if possible and if practical.
  - Periodically review these practices and procedures and revise as needed (re-train as needed and re-communicate these standards as needed).

<u>Suspicious Mail</u>: Characteristics of suspicious mail include the following:

- No return address appears on the package.
- The package has oily or other types of stains on it, discolorations, or a crusty substance or crystallization on it.
- Tape, staples or string are used in excess apparently to keep the package together.
- The package is oddly shaped or uneven.
- The package is very stiff or rigid or is bulky.
- The package has a peculiar odor.
- Words have been misspelled.
- The package is not addressed to a named individual, but is addressed to a title.

Handling Suspicious Mail: In the event mail is found to be suspicious, recommendations include:

- Looking for suspicious mail indications (such as those listed above) and treating the package as suspicious.
- Immediately isolating the package.
- Handling it with care.
- Not shaking, dropping, or bumping the package.
- Not opening it.
- Not smelling it.
- Alerting the company's crisis management team and/or calling law enforcement authorities.
- Using protective gloves when handling.
- Thoroughly washing hands with soap and water after handling the package.

Special Instructions: Furthermore, should a threat be identified, take the following precautionary measures:

- For a Bomb: Immediately evacuate the area; call the company's crisis management team and/or local law enforcement authorities; contact U.S. Postal inspectors.
- For Radiological: Limit the length of time exposed to the substance and limit the number of people exposed to it; do not handle the package; evacuate the area; protect personnel and yourself from the package.
- For Biological or Chemical: Isolate the package; do not handle it; evacuate the immediate area; thoroughly wash hands with soap and water.

Conclusion: The safe and secure handling of mail has taken on greater significance of late. By following a practical and common sense approach to handling it, risk to property and personnel can be dramatically reduced.

Resources: Peruse the web sites listed below to obtain further recommendations and details concerning the safe and secure handling of mail:

- Government/Agency Sites
  - Bureau of Alcohol, Tobacco and Firearms (BATF): www.atf.treas.gov
  - Centers for Disease Control (CDC): www.cdc.gov
  - Federal Bureau of Investigation (FBI): www.fbi.gov
  - General Services Administration (GSA): www.gsa.gov
  - Occupational Safety and Health Administration (OSHA): www.osha.gov
  - U.S. Department of Health and Human Services: www.hhs.gov
  - U.S. Postal Inspection Service and U.S. Postal Service: www.usps.com

APPENDIX D

International Security Notes: Self-Protection and Protection of Employees

(Outline prepared by Douglas B. Whiting, October, 2002 douglas.whiting@prodigy.net)

1. Preparation for overseas trip/assignment

a. vaccinations

b. medical travel clinic
- i. employee benefit or at employee cost?
- ii. Center for Disease Control
- iii. Melfloquine (malaria)
  test it out first!
- iv allergies / medication
- v. lomotil
- vi. Medi-vac coverage program

c. food
antiseptic wipes?
granola bars?
water? (lots of luck)
local doctors
embassy contacts

d. travel plans
- i if possible, make sure that you have a host who is taking care of you
  trip to India without limo
  - A. use airport greeters
    1. NO COMPANY NAMES
    2. Use alias or nickname?
- ii know where you're going -- don't get lost!
  trip to Indonesia --

2. travel tips

a. tips to avoid jet lag
- i. no heavy meals
- ii. no alcohol
- iii. no carbonated drinks
- iv. drink lots of water

b. adapters for electronic goodies?
- i adapter plugs
- ii adapter phone line jacks
- iii local access numbers for long distance carrier

c. do not put company name on luggage (don't use business cards); have a flop over your name on luggage

3. In-Country Security

a telephone calls and receipt of faxes – assume no confidentiality

b. receipt of emails

c. electronic eavesdropping in hotel rooms and conference rooms

d. sightseeing?

e. transportation to meetings and other engagements

f. how to arrange for "personal" delivery of closing checks where wire transfers are not practicable
   i. arrange for meeting points
   ii. arrange for message points

g. publicity – do you really want the media to publish that you are in town?

h. keep travel itineraries confidential – "our return flights are open"

i. no not get locked into a set routine (including travel paths)

j. avoid narrow streets where you could be blocked off

k. have plenty of hidden cash – use a money belt

l. alternatives to jogging on the streets
   is it acceptable for women to jog on the streets?

j. keep that U.S. passport hidden!

k. face up to risks associated with ANY sexual encounters

l. become aware of the local scams and tricks

m. watch on right hand if driving and in crosswalks in U.K. and other driver-on-right countries

n. keep gas tank at least _ full at all times

o. do not attract attention to yourself

p. obtain and carry cell phone for international assignments

q. for long-term assignments, stockpile first aid supplies, prescription medications, food, and bottled water – at least a 30-60 day supply.

APPENDIX E

A QUESTIONNAIRE ON KEY SECURITY CONCERNS

Corporate Security and Emergency Planning

1. Does your company have a formal corporate security policy? Yes___ No___

2. Does your company have a formal crisis management policy or emergency preparedness plan? Yes___ No___

3. Has either been re-evaluated since 9/11? Yes___ No___

4. If you have re-evaluated the plan since 9/11, do you know what risks are most critical to your business and where you are vulnerable? Yes___ No___

5. Are the implications of these risks reflected in strategic and operating plans? Yes___ No___

6. If you are a multi-national corporation, do you have a corporate security and emergency response plan in place for every one of your offices? Yes___ No___

7. Does your plan cover:

    a. Workplace violence (assaults, bombs, hostage taking)? Yes___ No___
    b. Environmental hazards (spills, leakage, other accidents)? Yes ___ No___
    c. Natural disasters (fire, earthquake, flood)? Yes___ No___
    d. Public infrastructure disruption (power, telecom, transportation)? Yes___ No___
    e. Penetration of computer facilities (system breakdown, network intrusion, denial of service)? Yes___ No___
    f. Major theft of intellectual property Yes___ No___
    g. Political and civil emergencies (change of government, war, terror attack)? Yes ___ No___
    h. Mail handling? Yes___ No___

8. Does your company have programs in place for

    a. Perimeter Control (access to the exterior border or campus of company property)? Yes___ No___
    b. Building Access Control? (access to individual buildings)? Yes___ No___
    c. Interior Access Control? (access to restricted areas within buildings - server locations, telephone facilities, hazardous material sites, laboratories, executive offices, etc.)? Yes___ No___

9. Do you test your corporate security and emergency response plans, using exercises such as penetration tests of buildings, secure areas, computer systems, or emergency drills? Yes___ No___
10. Does your company use electronic card access? Yes___ No___

11. Does your company use closed circuit television? Yes___ No___

12. In the event of an emergency, does the company's emergency plan make clear

    a. The chain of command - who will be in charge during a emergency in each location? Yes___ No___
    b. Who will comprise the emergency management team? Yes___ No___
    c. Who will communicate and how with the employees, employees' families, the public, law enforcement and civil authorities? Yes___ No___
    d. Where employees and outside parties can be report and obtain information? Yes___ No___
    e. Key contact telephone numbers and web sites? Yes___ No___
    f. Emergency evacuation, escape and rescue policies? Yes___ No___
    g. Defined levels of emergency conditions (e.g. at what point buildings will be evacuated; law enforcement notified)? Yes___ No___
    h. How employees and their families will be evacuated from a building, a work site or country? Yes___ No___

13. Does the plan cover every company office and facility around the world? Yes___ No___

12. Is the plan graded according to levels of urgency? Yes___ No___

13. Do designated emergency team leaders have information on

    a. Locations of keys, cards and codes to buildings and facilities? Yes___ No___
    b. 24/7/365 contact information for key people (senior executives, MIS, corporate security, human resources, public relations, local police, special consultants) Yes___ No___

Pre-employment Background Investigations

1. Does your company conduct pre-employment background investigations? Yes___ No___

2. Does your pre-employment background investigation policy apply to

    a. All hires? Yes___ No___
    b. Just certain classifications of hires? Yes___ No___

3. Do your pre-employment background investigations cover

    a. At least 15 years prior to employment? Yes___ No___
    b. Criminal history? Yes___ No___
    c. Judgments, liens and bankruptcy? Yes___ No___
    d. Regulatory violations? (e.g. SEC) Yes___ No___
    e. Verification of prior employment? (including title, salary, term of service)?

Yes___ No___

f. Verification of academic degrees? Yes___ No___

Vendor Integrity

1. Do you have a "Know Your Customer" policy? Yes___ No___

2. Do you have a "Know your Vendor" policy? Yes___ No___

3. Do you conduct background investigations of vendors? Yes___ No___

4. Do you conduct due diligence investigations of counter-parties in joint ventures, partnerships and other business combinations? Yes___ No___

5. In your ex-United States locations, have your verified the backgrounds and reputations of companies and individuals to whom you sell or from whom you buy goods and services? Yes___ No___

Corporate Internal Investigations

1. Do your employees have a confidential means, such as a hotline, to notify management of crime or misconduct? Yes___ No___

2. If you needed to search electronic files for evidence of crime or misconduct

   a. Does your company maintain a record of the location and assignment of all desktop and laptop computers? Yes___ No___
   b. Is data (including email) routinely backed up to a server and stored for a minimum of 12 months? Yes___ No___
   c. Does your telephone system store records of numbers dialed from individual telephone extensions? Yes___ No___
   d. re card reader system records maintained and backed up? Yes___ No___

American Corporate Counsel Association
Annual Meeting, October 23, 2002

Security Concerns for Global Business

Daniel E. Karson
Executive Managing Director and Counsel
Kroll Associates

A Questionnaire on Key Security Concerns

Corporate Security and Emergency Planning

1. Does your company have a formal corporate security policy? Yes___ No___

2. Does your company have a formal crisis management policy or emergency preparedness plan? Yes___ No___

3. Has either been re-evaluated since 9/11? Yes___ No___

4. If you have re-evaluated the plan since 9/11, do you know what risks are most critical to your business and where you are vulnerable? Yes___ No___

5. Are the implications of these risks reflected in strategic and operating plans? Yes___ No___

6. If you are a multi-national corporation, do you have a corporate security and emergency response plan in place for every one of your offices? Yes___ No___

7. Does your plan cover:

    a. Workplace violence (assaults, bombs, hostage taking)? Yes___ No___
    b. Environmental hazards (spills, leakage, other accidents)? Yes ___ No___
    c. Natural disasters (fire, earthquake, flood)? Yes___ No___
    d. Public infrastructure disruption (power, telecom, transportation)? Yes___ No___
    e. Penetration of computer facilities (system breakdown, network intrusion, denial of service)? Yes___ No___
    f. Major theft of intellectual property Yes___ No___
    g. Political and civil emergencies (change of government, war, terror attack)? Yes ___ No___
    h. Mail handling? Yes___ No___

8. Does your company have programs in place for

    a. Perimeter Control (access to the exterior border or campus of company property)? Yes___ No___

b. Building Access Control? (access to individual buildings)? Yes___ No___
c. Interior Access Control? (access to restricted areas within buildings - server locations, telephone facilities, hazardous material sites, laboratories, executive offices, etc.)? Yes___ No___

9. Do you test your corporate security and emergency response plans, using exercises such as penetration tests of buildings, secure areas, computer systems, or emergency drills? Yes___ No___

10. Does your company use electronic card access? Yes___ No___

11. Does your company use closed circuit television? Yes___ No___

12. In the event of an emergency, does the company's emergency plan make clear

a. The chain of command - who will be in charge during a emergency in each location? Yes___ No___
b. Who will comprise the emergency management team? Yes___ No___
c. Who will communicate and how with the employees, employees' families, the public, law enforcement and civil authorities? Yes___ No___
d. Where employees and outside parties can be report and obtain information? Yes___ No___
e. Key contact telephone numbers and web sites? Yes___ No___
f. Emergency evacuation, escape and rescue policies? Yes___ No___
g. Defined levels of emergency conditions (e.g. at what point buildings will be evacuated; law enforcement notified)? Yes___ No___
h. How employees and their families will be evacuated from a building, a work site or country? Yes___ No___

13. Does the plan cover every company office and facility around the world? Yes___ No___

12. Is the plan graded according to levels of urgency? Yes___ No___

13. Do designated emergency team leaders have information on

a. Locations of keys, cards and codes to buildings and facilities? Yes___ No___
b. 24/7/365 contact information for key people (senior executives, MIS, corporate security, human resources, public relations, local police, special consultants) Yes___ No___

Pre-employment Background Investigations

1. Does your company conduct pre-employment background investigations? Yes___ No___

2. Does your pre-employment background investigation policy apply to

    a. All hires? Yes___ No___
    b. Just certain classifications of hires? Yes___ No___

3. Do your pre-employment background investigations cover

    a. At least 15 years prior to employment? Yes___ No___
    b. Criminal history? Yes___ No___
    c. Judgments, liens and bankruptcy? Yes___ No___
    d. Regulatory violations? (e.g. SEC) Yes___ No___
    e. Verification of prior employment? (including title, salary, term of service)? Yes___ No___
    f. Verification of academic degrees? Yes___ No___

Vendor Integrity

1. Do you have a "Know Your Customer" policy? Yes___ No___

2. Do you have a "Know your Vendor" policy? Yes___ No___

3. Do you conduct background investigations of vendors? Yes___ No___

4. Do you conduct due diligence investigations of counter-parties in joint ventures, partnerships and other business combinations? Yes___ No___

5. In your ex-United States locations, have your verified the backgrounds and reputations of companies and individuals to whom you sell or from whom you buy goods and services? Yes___ No___

Corporate Internal Investigations

1. Do your employees have a confidential means, such as a hotline, to notify management of crime or misconduct? Yes___ No___

2. If you needed to search electronic files for evidence of crime or misconduct

    a. Does your company maintain a record of the location and assignment of all desktop and laptop computers? Yes___ No___
    b. Is data (including email) routinely backed up to a server and stored for a minimum of 12 months? Yes___ No___
    c. Does your telephone system store records of numbers dialed from individual telephone extensions? Yes___ No___
    d. Are card reader system records maintained and backed up? Yes___ No___

International Security Notes: Self-Protection and Protection of Employees

(Outline prepared by Douglas B. Whiting, October, 2002 douglas.whiting@prodigy.net)

1. Preparation for overseas trip/assignment

a. vaccinations

b. medical travel clinic
- i. employee benefit or at employee cost?
- ii. Center for Disease Control
- iii. Melfloquine (malaria)
  test it out first!
- iv allergies / medication
- v. lomotil
- vi. Medi-vac coverage program

c. food
antiseptic wipes?
granola bars?
water? (lots of luck)
local doctors
embassy contacts

d. travel plans
- i if possible, make sure that you have a host who is taking care of you
  trip to India without limo
  - A. use airport greeters
    1. NO COMPANY NAMES
    2. Use alias or nickname?
- ii know where you're going -- don't get lost!
  trip to Indonesia --

2. travel tips

a. tips to avoid jet lag
- i. no heavy meals
- ii. no alcohol
- iii. no carbonated drinks
- iv. drink lots of water

b. adapters for electronic goodies?
- i adapter plugs
- ii adapter phone line jacks
- iii local access numbers for long distance carrier

c. do not put company name on luggage (don't use business cards); have a flop over your name on luggage

3. In-Country Security

a telephone calls and receipt of faxes – assume no confidentiality

b. receipt of emails

c. electronic eavesdropping in hotel rooms and conference rooms

d. sightseeing?

e. transportation to meetings and other engagements

f. how to arrange for "personal" delivery of closing checks where wire transfers are not practicable
   i. arrange for meeting points
   ii. arrange for message points

g. publicity – do you really want the media to publish that you are in town?

h. keep travel itineraries confidential – "our return flights are open"

i. no not get locked into a set routine (including travel paths)

j. avoid narrow streets where you could be blocked off

k. have plenty of hidden cash – use a money belt

l. alternatives to jogging on the streets
is it acceptable for women to jog on the streets?

j. keep that U.S. passport hidden!

k. face up to risks associated with ANY sexual encounters

l. become aware of the local scams and tricks

m. watch on right hand if driving and in crosswalks in U.K. and other driver-on-right countries

n. keep gas tank at least _ full at all times

o. do not attract attention to yourself

p. obtain and carry cell phone for international assignments

q. for long-term assignments, stockpile first aid supplies, prescription medications, food, and bottled water – at least a 30-60 day supply.

Reach Over 13,000 In-house Counsel—Free!

When members of the American Corporate Counsel Association/Global Corporate Counsel Association have a practice issue they need advice on, they turn to the association. Now, they have a new association resource to rely on when they seek to retain outside counsel: **InternationalCounsel,** a database of outside counsel who practice outside the United States. Put your qualifications before the over 13,000 in-house counsel who are members of the American Corporate Counsel Association/Global Corporate Counsel Association. Post your information online—at no cost to you—at **www.internationalcounsel.org.**

ACCA
American Corporate Counsel Association
Global Corporate Counsel Association

The in-house bar association℠ 1025 Connecticut Avenue, NW Suite 200 Washington, DC 20036-5425 202.293.4103 www.acca.com