TOP THREE INTERNATIONAL CONCERNS FOR DIRECTORS AND OFFICERS

by Ann Longmore, December 13, 2013

Last month, I had the distinct honor and pleasure to participate in a panel discussion at the Professional Liability Underwriting Society’s 26th Annual PLUS International Conference on Global D&O: Navigating the Exposures of Multinational Companies. For me, it sparked a moment of reflecting on how far we’ve come in our appreciation and understanding of the challenges facing today’s global executive as well as the opportunity to speculate on what is still to come.

During the wide-ranging conversation, the panelists targeted three major areas of risk facing today’s global executives.

THE COURT OF PUBLIC OPINION: LITIGATION VS. REPUTATION

Fortunately, we didn’t have to begin the discussion by first persuading those in attendance that there actually were global exposures – meaning risks outside the U.S. – facing executives and firms today. This was a given for the audience and the panel.

Rather, fellow-panelist Lanny J. Davis, of Lanny J. Davis & Associates, kicked us off describing a new world order where companies and individuals are tried first in the “courts” of social media, where the rules of law and the conventions of good journalism may not apply. In these forums, personal reputations, a company's stock price and a global brand are all at risk.

Critically, for several of us on the panel, while directors and officers (D&O) liability insurance is designed to respond to the ensuing litigation, it does little to repair reputations. I have long been a proponent of D&O policy extensions designed expressly to provide media relations coverage, and Lanny’s able and passionate advocacy for legal crisis response reminded us all that there is more, potentially much more, to a successful outcome than winning at trial – assuming the issues are ever tried before a judge or a jury.

MORRISON GLOBALIZES LITIGATION

A few years back, the U.S. Supreme Court issued a decision seen as a godsend to many an international organization in Morrison v National Australia Bank. The result of this was to deny access to the U.S. courts for cases where non-U.S. shareholders had purchased shares of non-U.S. companies on non-U.S. exchanges (the so-called F-cubed cases). U.S. shareholders holding shares purchased in the U.S. could get their day in a U.S. court—but all others where potentially “deported” to other jurisdictions.

The result of Morrison, in part, has been more local D&O litigation around the globe—as vividly illustrated by a map of today’s “hot” countries for companies and executives, presented by fellow panelist Edward Smerdon, a partner at Sedgwick Detert Moran & Arnold. His map provided a thought-provoking trip round the world—though Ed did clarify that the only truly red “hot” country was the U.S., which was not highlighted on our map. The other countries really being more appropriately viewed as “tepid” jurisdictions in comparison. But with the focus of the session on non-U.S. risks, the U.S. of A. was not part of our briefing.

BOARDS GONE GLOBAL (REALLY)

Fellow panelist Chris Magee, a Managing Partner of Berkley Professional Liability UK, and I were in agreement about the interesting result of U.S. companies re-domiciling abroad (outside the U.S.) while keeping their U.S. securities listing and shareholder base: as the local sister companies of the U.S. underwriters are seen to offer the same or better terms and conditions of coverage at significantly discounted rates.

CONTENT:

Top three International Concerns for Directors and Officers...............1
U.S. Proposes Cyber Security Standards but Adoption Remains the Wildcard........................................2
The EEOC Goes Trolling.................................................................................................................3
SEC as Beat Cop, Enforcing “Our Federal Securities Laws, Big and Small…”....................................3
A true win-win for the buyers, many of whom are often confused by this turnabout as they do not perceive their inherent exposures as significantly decreasing due to a change in the country of domicile of the parent organization. Rather, they realistically see their risks as the U.S. plus an overlay of requirements and potential liability arising from their new local abode.

All in all, at least for those of us on the panel, it was an interesting and thought-provoking session.

U.S. PROPOSES CYBER SECURITY STANDARDS BUT ADOPTION REMAINS THE WILDCARD

by Christopher Keegan, November 6, 2013

The National Institute of Standards and Technology’s (NIST) recently published their latest draft of the preliminary cybersecurity framework—a set of voluntary standards that companies can adopt to boost cyber security.

The draft framework, which NIST was directed to develop by the Obama administration, was published after input from thousands of critical infrastructure organizations, academics, security specialists and the insurance industry—including Willis.

The framework is part of an attempt to protect critical industries—such as financial institutions and power grids, from potentially crippling cyber attacks or national security threats, without enacting overly restrictive and costly laws. Essentially, the framework aims to turn current “best practices” into accepted standards that can be applied to reduce threats. Perhaps more importantly, the framework intends to be nimble—a living, breathing document—that can evolve to keep pace with the rapidly moving risks.

SETTING THE STANDARD

The draft framework proposes five core functions in keeping information and systems safe:

1. Identify risks
2. Protect systems
3. Detect attacks
4. Respond to incidents
5. Recover afterwards

Specifically, the framework lays out guidance for companies on techniques to influence their cyber risk “outcomes.”

The framework also addresses best practices on the communication of cyber risk across organizations and provides “implementation tiers” to allow companies to benchmark their risk management practices. The benchmarking standards include determining the acceptable level of risk, developing measures of risk tolerance and maturity of risk management practices, creating a target risk profile and a framework core—a set of specific practices which are to be developed and followed.

In Willis’ view the framework is a great start because it features the input of industry groups. It will likely improve further when the final version is issued in February. Even though it lacks specific requirements the draft framework aligns with many current network and cyber risk audit standards currently used. In addition, the framework could develop into a strong resource for companies and industries that have yet to implement a cyber risk audit.

COLLABORATION OR REGULATION

Some improvements to the framework may need to be made to provide specific baseline standards and differentiation for industry verticals. Much will depend upon the process that NIST and the Department of Homeland Security put in place to encourage companies to share data. If consensus standards are not developed we may see the DHS take a more aggressive approach via regulation—an approach that may not be constructive.

During Willis’ discussions with NIST at the White House on August 26th and in subsequent discussions with Senate staff, Willis was informed that it is the intention of the White House to hand the Framework over to the DHS, but it’s not clear exactly what role they would play. There was also discussion around the industry that some organizations might get a safe harbor from litigation if they follow the framework. From our discussions with legislators, we do not believe this safe harbor will be in the final version of the framework.

Industry reaction to the framework thus far has been guardedly positive largely because many firms’ have been able to influence the framework standards to align with many currently accepted practices.

As with any new set of guidelines, adoption remains the true test of success. We expect those industries in the critical sectors who already have audit standards in place similar to the framework, to be the first to abide by the framework standards. Beyond that, pressure from government departments and the U.S. Securities and Exchange Commission, combined with the threat of regulation and litigation is likely to increase compliance with the final framework standards.
THE EEOC GOES TROLLING
by Ann Longmore, December 13, 2013

In what appears to be a first for the Equal Employment Opportunity Commission (EEOC), the Commission used a mass email to 1,330 current and former employees of a company under an age discrimination investigation in order to solicit assistance in their investigation. The email contained a link to a questionnaire that included such questions as:

- “At any point during the application process, did anyone ... make any comments about your age?”
- “At any point during the application process, did anyone ... make any comments about the age of applicants/employees?”
- “At any point during the application process, did anyone ... make any other age-related comments?”

QUESTIONABLE TACTICS

The Commission had access to the email addresses because the company had voluntarily provided them as part of its response to an EEOC’s request for information that accompanied a letter announcing that the EEOC was opening a nationwide investigation under the Age Discrimination in Employment Act (ADEA). A year and a half later, the company’s employees and managers received the email blast.

YOUR MOVE

In response, the company filed a lawsuit against the EEOC. It alleged that the Commission violated the federal

Administrative Procedure Act as well as the company’s constitutional rights under the Fourth Amendment search and seizure clause and the Fifth Amendment takings clause for the agency’s unauthorized use of CNH’s computer data and its unannounced, ex parte investigative communications with the company's management.

The suit seeks copies of all information gathered by the Commission through their emailed questionnaire and to permanently bar the EEOC from utilizing this information in any subsequent lawsuit the EEOC may commence against the firm.

Meanwhile, the EEOC has defended its actions as falling within the EEOC’s investigatory power to communicate with employees. The Commission has sought to have the company’s suit over its tactics dismissed, stating:

While the content of the email communication may have caused discussion among employees and managers at the workplace, communication by face-to-face, regular mail or telephone could have had the same impact on the persons contacted... Investigations by federal agencies may disrupt the processes of normal business operations but this is the cost of doing business and does not result in a cognizable harm.

Stay tuned to see how the EEOC fares with its new tactics.

SEC AS BEAT COP, ENFORCING “OUR FEDERAL SECURITIES LAWS, BIG AND SMALL...”
by Ann Longmore, December 25, 2013

We recently wrote about some new enforcement principals and strategies of the U.S. Securities and Exchange Commission. But it may have escaped notice that the SEC is apparently not going to focus on potentially significant violations in terms of size or investors affected, but rather intends to police violation of all sizes. We know this because they have told us so.

AN OVERARCHING PRINCIPLE: COVER THE WHOLE MARKET

“One of our goals is to see that the SEC’s enforcement program is – and is perceived to be – everywhere, pursuing all types of violations of our federal securities laws, big and small.” – SEC Chair Mary Jo White

In fleshing out the comments that the SEC Chair had made a few weeks earlier on the topic of enforcement, there was a repeat of the theme of the Commission as a “strong cop on the beat,” adding that they will not be “just someone sitting in the station house waiting for a call, but patrolling the streets and checking on things.”

The SEC will therefore not ignore apparent minor violations in favor of the big one that come with media attention. The Chair of the SEC then went on to compare this approach to that of a former mayor of New York City who pursued violations involving “street corner squeegee men to graffiti artists to subway turnstile jumpers to the biggest crimes in the city.”
RESOURCE ALLOCATION
How to be everywhere at all times, especially with resource limitations? The SEC has a four-step plan:

1. By emphasizing the strength of the SEC’s exam program and combining this with incentives for individuals (whistleblowers) to step forward, then, collaborating with other enforcement agencies combined with the SEC’s technological capabilities.
2. Focusing on “deficient gatekeepers.”
3. By not overlooking the small violations to avoid an environment of indifference to the law.
4. Continuing to highlight the bigger cases by seeking to punish major offenses to act as a deterrence to bad actors while boosting investors confidence.

INCENTIVES FOR INDIVIDUALS – AKA WHISTLEBLOWERS
Dodd-Frank established the SEC’s whistleblower bounty program. With the 3rd bounty recently announced, the SEC categorizes the bounty program as, “...a tremendously effective force-multiplier, generating high quality tips and, in some cases, virtual blueprints laying out an entire enterprise, directing us to the heart of an alleged fraud.” Those are strong words.

The existence of the bounty program may be responsible for companies improving the internal audit and compliance function and better treatment for those who report potential wrongful conduct internally. An important note here is that the SEC tells us, “most in-house whistleblowers that come to us went the internal route first.”

GATEKEEPERS BEWARE
The SEC’s focus on “delinquent” gatekeepers is a bit chilling. For in addition to certain organizations this group may well include in-house and outside counsel.

SUGGESTED READING
While our October Alert spoke to “required reading,” this more recent speech from the SEC is certainly worth reading as well: Remarks at the Securities Enforcement Forum.

continued from page 3