

Insider Threats to Critical Infrastructures

We often hear about reports and recommendations issued by agencies and private groups analyzing issues of importance to business and government. Somewhat lost in this election year was a report issued in April 2008 by the National Infrastructure Advisory Council (NIAC), which provides the President and the Department of Homeland Security (DHS) with "advice on the security of the critical infrastructure sectors and their information systems."¹ The NIAC includes members from manufacturing and technology industries, utilities, law enforcement, government, and academia. The critical infrastructures addressed by the NIAC support vital sectors of the economy including transportation, energy, finance, and manufacturing.

This topic is a natural follow-up to last issue's discussion of business continuity planning. This article and the report it discusses address a number of issues that business and government need to focus on in evaluating potential insider threats.

The study was initiated in early 2007 by DHS Secretary Michael Chertoff, assigning to the NIAC the task of defining the insider threats for both physical and virtual infrastructures. The special focus of this study was to address insider threats that exist in all organizations, including the potential for acts of sabotage, theft, or violence in the workplace. As part of the detailed findings in this 55-page report, "the NAIC defined the insider threat to critical infrastructure as *one or more individuals with the access and/or insider knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm.*"²

The report identified a series of problems involving employee screening, potential for economic sabotage, the reason that insiders may cause a threat to critical infrastructures, and the dynamics associated with technol-

ogy and globalization. In its letter to the President, the NIAC summarized its recommendations for actions by government and business as follows:

- **Executive leadership awareness.** Recommendations and a framework approach for improving executive leadership awareness of the insider threat to critical infrastructures. The recommendations include a request for White House leadership on executive awareness to coordinate government efforts and engage with critical infrastructure executive leadership on this important issue.
- **Employee screening and risk assessments.** Detailed findings and recommendations to improve critical infrastructure operator employee screening and risk assessments. The NIAC's recommendations concur with the recommendation in the 2006 Attorney General's Report on Criminal History Background Checks to expand private sector use of federal criminal history sheet records, while preserving existing privacy protections that flow from the Fair Credit Reporting Act for most current private-sector background checks.
- **Role for DHS and Sector Coordinating Councils.** The Department of Homeland Security and the Sector Coordinating Councils (SCCs) should support critical infrastructure operators in developing insider threat risk assessments, insider threat policies, and risk mitigations.
- **Technology policy.** Recommendations for improved technology policy to help critical infrastructure operators address the emerging information technology (IT) dynamic to the insider threat.
- **Information sharing.** Recommendations to improve insider threat risk assessments through

information sharing, both among owners and operators in each sector and also with government on research and intelligence.

- **Future research.** The NIAC identified key focus areas for future research on challenges presented by globalization, technology threats and solutions, and personnel risk assessments, where time, resources, and a current understanding of the insider threat limited specific policy recommendations.³

The findings and recommendations of this report should serve as a wake-up call for business and government to address potential insider threats and be proactive to ensure that critical infrastructures in the United States are protected.

NOTES

1. Page 4 of The National Infrastructure Advisory Council's Final Report and Recommendations on the Insider Threat to Critical Infrastructures, April 8, 2008. http://www.isalliance.org/images/stories/2008MissedIt/August08/niac_insider_threat_to_critical_infrastructures_study.pdf

2. Page 5, Advisory Council Report, *supra*.

3. Letter dated June 23, 2008 from the National Infrastructure Advisory Council to the President. http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_letter.pdf



Michael S. Khoury, of Jaffe Raitt Heuer & Weiss, PC, Ann Arbor and Southfield, practices in the areas of information technology, electronic commerce, intellectual property, and commercial and corporate law. He is the past chairperson of the State Bar of Michigan Business Law Section and past chairperson of the Computer Law Section. He is also a member of the American Bar Association Sections of Business Law, Science and Technology, and Intellectual Property.