New From NUJIA

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor, Information Assurance
Norwich University, Northfield VT

The Norwich University Journal of Information Assurance <http://nujia.norwich.edu> has some new postings that readers may be interested in reading. The NUJIA is a peer-reviewed professional journal focusing on scholarly papers that are useful to working information assurance practitioners. The PDF files are freely downloadable but we request that no one re-post them on a public site (so that we can easily make corrections as necessary without chasing down duplicates).

***

"An Introduction to Factor Analysis of Information Risk (FAIR): A framework for Understanding, Analyzing, and Measuring Information Risk," by Jack A. Jones, CISSP, CISM, CISA. Mr Jones, a CISO with 22 years of experience in information technology, argues that the lack of well-defined terminology interferes with our credibility in our organizations. He explores concepts of risk and risk management and challenges received wisdom with his interesting approach to the precise analysis and description of risk. I was particularly taken with his introductory challenge – the “Bald Tire Scenario” – where he poses the following questions (quoting):

As you proceed through each of the steps within the scenario below, ask yourself how much risk is associated with what’s being described.

- Picture in your mind a bald car tire. Imagine that it’s so bald you can hardly tell that it ever had tread. How much risk is there?
- Next, imagine that the bald tire is tied to a rope hanging from a tree branch. How much risk is there?
- Next, imagine that the rope is frayed about halfway through, just below where it’s tied to the tree branch. How much risk is there?
- Finally, imagine that the tire swing is suspended over an 80-foot cliff – with sharp rocks below. How much risk is there?

Now, identify the following components within the scenario. What were the:

- Threats
- Vulnerabilities
- Risks.

You will enjoy reading his analysis of the errors that continually crop up in discussions of this scenario.

***

Another interesting paper on the NUJIA Web site is “Litigation Management as Part of a Comprehensive Compliance Management Program,” by Keith D. Willett, MSIA, CISSP-ISSAP. Mr Willett is “a Principal Computer Scientist for Computer Sciences Corporation’s (CSC’s) Global Security Solutions (GSS) Department … [and]… performs the tasks of a security"
architect for CSC’s commercial, federal, intelligence, and defense clients….” He was also the valedictorian in his graduating class from the MSIA program in 2005. Mr Willett presents practical advice on what to do if – Heaven forfend – one’s organization should end up in court charged with violations of regulatory requirements. Such planning should be part of one’s disaster prevention, mitigation and recovery processes.

* * *

“Legal Implications of Warfare in the Information Age,” by Cory Mazzola, MSIA, CISSP, CPM, MCSE is a short and thought-provoking essay about the growing interdependence of organizations all over the world – in the absence of a sound international legal framework for governing electronic misbehavior. Mr Mazzola writes, “In the absence of legal hurdles preventing and penalizing illegitimate actions, rogue states face little incentive to scuttle self-serving IW programs. International agreements and restrictions must restrain states from recklessly pursuing offensive programs at the expense of fellow nations. We need legal parameters to guide logical and legislative actions on a national and transnational plain. We must lay a foundation through domestic and international legal initiatives, armed with incentives and sanctions, to provide political and technological solutions while legitimizing avenues of approach and formal engagement.” Mr Mazzola has an extensive background in communications security and network defense as an officer in the US Air Force.

* * *

The NUJIA welcomes original papers from all sources for consideration and I encourage readers with the time and interest to write thoughtful essays with appropriate references for further reading to consider our journal as a useful place to reach information assurance professionals.

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.