You Cannot Pass the Buck on Reliable Network Security

Who has the responsibility within your organization to ensure that the network everyone has come to rely upon stays operational? Typically, you may respond: "Oh, that is taken care of by our network administrator. They stay on top of that. That is why we pay them the *big bucks!*" Unfortunately, as we learn from Moira West-Brown in *Avoiding the Trial-by Fire Approach to Security Incidents*, "Most organizations do not even think of how to respond to a computer security incident until after they have experienced a significant one."

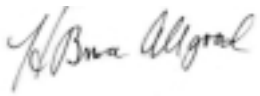
Most of us probably do not care to know what is being done to keep our networks up until we are affected personally. How many of us were *not* impacted in some way by the recent Love Letter e-mail virus attack? West-Brown also points out that insurance coverage for security losses will likely be changing. Some insurance companies offer financial protection for third-party damages resulting from security breaches. However, she says, "It is only a matter of time before insurance companies begin to request more information about network security, and begin to raise the cost of general insurance coverage for companies that are ill prepared to detect and respond to computer-security incidents."

Networks have become indispensable for conducting business everywhere—in government, industry, and your organization. Networked systems allow access to needed information rapidly, improving communications while reducing costs. This reduction in costs, however, could be easily overshadowed by the cost of security breaches as indicated in *Improving the Security of Networked Systems*, by Julia Allen, et al. They note that security breaches are on the rise, and the cost is increasing. Financial losses for reporting organizations have doubled to more than $265 million according to a recent survey. Is your organization at risk? How would you know? Read this article and discover that the goal of OCTAVE[SM] [1] is "to improve how well information assets are protected, putting organizations in a better position to achieve their missions." OCTAVE enables organizations to develop appropriate protection strategies by considering policy, management, administration, and other organizational issues, as well as technologies, to form a comprehensive view of the information security state of that organization.

Another method providing a systematic means to assess and improve system survivability for risk reduction is described in *The Survivability Imperative: Protecting Critical Systems* by several authors of the Software Engineering Institute. Our modern society is increasingly dependent upon complex network environments. Complex systems may improve efficiency, but they also introduce additional intrusion risks by unknown parties with destructive motivations. These risks can be mitigated by incorporating survivability capabilities, according to the authors. "Survivability analysis is a prudent risk management technique in a world that increasingly depends on complex, large-scale network systems," they conclude.

An interesting perspective on some of the challenges we face in taking full advantage of the electronic capabilities to streamline government and consumer/customer service is outlined in *Electronic Commerce and Governance: A Darwinian Discussion* by Nancy Lee Hutchin. She addresses learning to deal with removing personal feedback in online service relationships. How much are we willing to trust someone we cannot look in the eye? How do we evaluate trustworthiness? Are we willing to change the way we do business for time savings or convenience?

Several of this month's articles also mention the use of best practices as outlined in one of the Capability Maturity Models (CMMs). In *Avoid Self-Inflicted Wounds in Applying CMM to ATP Maintenance and Support*, David Putman discusses how to apply CMM concepts to hardware and software engineering. Rick Hefner, Ron Knode and Mary Schanken's article *The Systems Security Engineering CMM* describes essential characteristics of an organization's process required for good security engineering. In her article, Hutchin highlights the quantifiable business benefits achievable in moving from CMM level one to CMM level three. As a member of the CMM integrated product development team for more than two years, I enthusiastically recommend your continued interest in use of CMMs in all of your information technology process improvement efforts. I hope this month's issue of **CrossTalk** will provide several new ideas to benefit your organization.



H. Bruce Allgood
Deputy Computer Resources Support Improvement Program Director

1. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a service mark of Carnegie Mellon University.