Standards Today

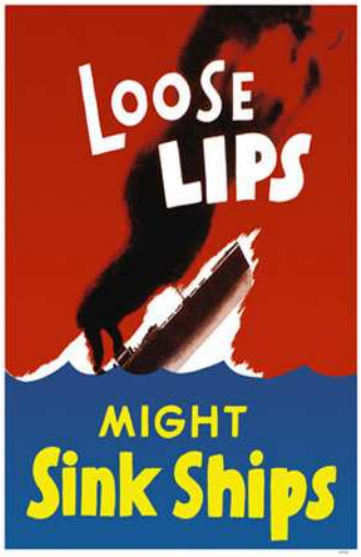
A Journal of News, Ideas and Analysis

A publication of
CONSORTIUM INFO.ORG
GesmerUpdegrove LLP

June-July 2009 Vol. VIII, No. 4

EDITOR'S NOTE:

Security – Then and Now



U.S. Department of War Information Office Poster - 1942

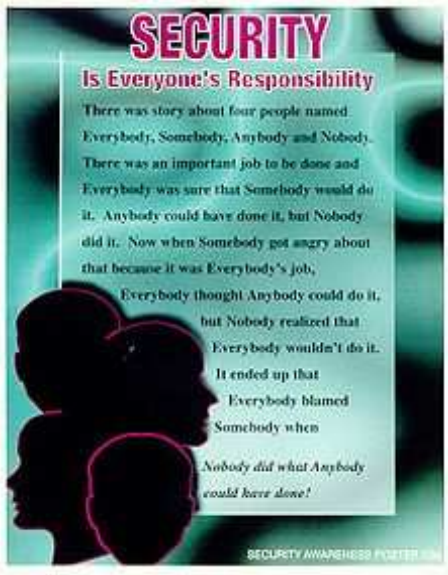
Security has always been a concern of government, doubtless from time immemorial, and especially in time of war. But until recently, ensuring security presented a much less difficult challenge – one that could be met with locks, guards, and ciphers against all but the most determined attackers.

Today, of course, that's all changed, and cybersecurity now demands attention in both the public and private sectors on a constant basis. With the danger of cyberattack becoming ever harder to ignore, the U.S. government has finally become alarmed, and is turning its attention to protecting both its own agencies as well as society at large from assaults launched by everyone from criminal hackers to rogue nations.

No surprise, then, that I am dedicating this issue of ***Standards Today*** to cybersecurity - yet another standards-dependent challenge that the Obama administration has pledged to address.

This issue is the fifth in a series I've written on such topics since the U.S. election, reflecting the heightened importance of standards and the standards development infrastructure to accomplishing key government initiatives (the prior issues were A Standards Agenda for the Obama Administration, The Electronic Health Records Standards Challenge, IT Policy and the Road to Open Government, and Standards and the Smart Grid).

In my ***Editorial*** this issue, I highlight how willing we are to deploy new technologies first, and only worry later about the risks that too often accompany them. In the ***Feature Article***, I offer a broad survey of the cybersecurity standards landscape, providing an overview of the challenges that our headlong rush into the virtual world has laid out our gates, the types of standards needed to address them, the organizations that are developing them, and the federal government's first steps in confronting its duty to protect itself, and society, from cyberattackers of all kinds.



U.S. Dept. of Commerce/Office of Security Awareness poster - 2009

In this month's ***Interview***, the PCI Security Standards Council's Bob Russo provides a detailed look into the operation of a unique organization. PCI SSC is dedicated to enabling the kind of unique, end-to-end, standards-based risk management infrastructure that is necessary to protect the private information of credit card and debit card users everywhere. It provides an important example of the type of holistic, collaborative approach that will be needed to address many other complex security challenges, in areas such as electronic health records, open government, and more.

Next, I provide an update on a situation that I have covered many times over the past five years, involving a chip designer called Rambus, and a standards development organization named JEDEC. Rambus has sometimes lost, but never failed to appeal, in the past in the multiple private suits and public investigations that have been launched against it – until now. In this, my latest ***Rambus Update***, I report on a recent settlement entered into between Rambus and the European Commission, and offer some thoughts on what might have motivated its uncharacteristic decision.

In my ***Standards Blog*** selection for this month, I describe an organization that was publicly launched a few weeks ago to promote the use of free and open source software by the U.S. federal government. That organization, appropriately enough, is called ***Open Source for America***, and I'm pleased to have been asked to serve on its Board of Advisors.

I close this issue, as usual, with a ***Consider This*** essay, this time mourning the lack of interest (so far) on the part of software designers, electronic publishers, and yes, standards developers, to embrace on line the Arts of the Book that have graced handwritten and printed texts for a full millennium. Hopefully, this will be only a temporary condition.

By way of disclosure, I should (and am proud to) note that I have served as legal counsel and/or have served on the Boards of Directors of the following standards organizations featured in this issue: ***American National Standards Institute***, ***Information Card Foundation***, ***Organization for the Advancement of Structured Information Systems (OASIS)***, ***OpenID Foundation***, ***PCI Security Standards Council***, and ***Messaging Anti-Abuse Working Group***. Any characterizations of these worthy groups included in this issue are mine alone, and should not be construed to have been authorized or made on behalf of any of these organizations.

As always, I hope you enjoy this issue. But whether you do or don't, it's always good to hear from you. You can reach me at andrew.updegrove@gesmer.com.

Andrew Updegrove
Editor and Publisher
2005 ANSI President's
Award for Journalism

The complete series of Consortium Standards Bulletins can be accessed on-line at http://www.consortiuminfo.org/bulletins/ It can also be found in libraries around the world as part of the EBSCO Publishing bibliographic and research databases