

Special Edition Lippis Report on Network Security | May 28, 2008

Network Security 2.0: A Systems Approach to Threat Mitigation Augments Defense in Depth

From the Publisher



Welcome to the first in a six part series on Network Security sponsored by Cisco Systems. We'll focus on a range of topics including "Managing Security Best Practices for PCI Compliance", "Cisco's role in identity management and access control", Securing the Data Center, Secure Mobility et al. This Lippis Report series includes exclusive podcasts, whitepapers, case studies and analysis to help business and IT leaders understand the new and more dangerous threats along with associated mitigation strategies.

In this first edition of the special series we focus on security architecture. The conventional wisdom in IT threat mitigation is to build a layered defense with security technology such as firewalls, IPS, network access control, anti-x client software, alarm aggregation and event correlation, etc. But conventional wisdom is shifting toward a systems approach to protecting IT assets. The systems approach builds upon IT security investment by wrapping it with System Management for policy, reputation and identity that transcend end-points, networks, content and application security. The systems approach promises to:

1. Enforce business policies and protect critical assets
2. Decrease IT/secops administration burden and reduce TCO
3. Reduce IT security and compliance risk

We explore this new defense approach with analysis, podcasts and case studies. Enjoy and we want your comments. Many of you send me your comments, but please post them on the lippis.com site so we can share with other subscribers and create dialog around these important topics.

Please visit and download sponsor content from lippis.com often, as it is due to the

generosity of their sponsorship that we are able to bring you this service.

[Read this Special Edition Lippis Report.](#)



Download Library Additions

Podcast

Network Security 2.0: Layered Security or Systems Approach?

The conventional wisdom in IT threat mitigation is to build a layered defense with security technology such as firewalls, IPS, network access control, anti-x client software, alarm aggregation and event correlation, etc. Conventional wisdom is starting to shift toward a systems approach to protecting IT assets. The layered approach was built upon deploying best-of-breed products, which were best-of-breed only until other products emerged and relegated them to either stand-alone appliances and/or loosely coupled silos such as the linking between IPS and firewalls. The systems approach builds upon IT security investment by wrapping it with System Management for policy, reputation and identity that transcend end-points, networks, content and application security. Fred Kost, Cisco's Director Security Marketing is my guest as we explain the new IT security model and provide IT leaders with guidance on building a more secure IT infrastructure.

[Listen to the podcast.](#)

Case Studies

University Virtually Eliminates Infections from Internal Users

By Cisco and Virginia Commonwealth University

Securing a network for any large organization is fraught with challenges. In a

university environment, however, where the need for security must be balanced with the need for academic freedom, those challenges can be even more complex. "Our security environment is very dynamic," says Mark Willis, chief information officer for Virginia Commonwealth University (VCU), a Richmond, Virginia-based university with 32,000 students and 10,000 faculty and staff. "At a regulatory level, we have increasing requirements to secure our networks and data. That is almost an anathema to an academic environment, which, by its nature, needs to be very open. We struggle to balance these needs and protect our assets from security risks."

The VCU network is far-flung and complex. The university stretches across two campuses, encompassing more than 140 buildings, 1800 network switches, more than 500 servers, and more than 42,000 users. Portions of the network connect with a large regional medical campus, meaning that many network segments must comply with strict data security regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and industry requirements such as protection of copyrighted materials. In addition, several areas of the university deal with credit card transactions and must meet Payment Card Industry (PCI) requirements. Although the university had long employed strong perimeter security, mitigating the risk from internal threats was a constant challenge.

[Find out how Mark Willis, VCU CIO did it by downloading this whitepaper.](#)

Building a Safer, Smarter State Government

By Cisco and State of Oregon

The state of Oregon is committed to improving the quality of life for all of its citizens. A national model for improving government, the state strives to deliver the highest level of service to its residents. More than 100 agencies are responsible for day-to-day government concerns such as education, public safety, human services, transportation, business, finances, and the environment. Information technology plays a key role in helping all of these agencies work efficiently, collaborate, and respond to constituents. Traditionally, each organization has been responsible for maintaining its own IT environment. Different systems and staff were dispersed across the state, each using its own business approach. However, this model left the state of Oregon vulnerable to network security issues that could bring government operations to a standstill.

[Find out how the state of Oregon closed network security vulnerabilities by downloading this whitepaper](#)

Community Bank Secures Data and Streamlines Regulatory Compliance

By Cisco and Premier Valley Bank

Premier Valley Bank (PVB) uses a Self-Defending Network and 24-hour monitoring from HEIT to create an adaptable, end-to-end defense system. Protecting against network attacks makes good sense for any business, but for financial services companies, it's not just a good idea it's the law. PVB must comply with a broad range of information security regulations from the Federal Financial Institutions Examination Council (FFIEC) and the California Department of Financial Institutions. In periodic audits, PVB must demonstrate that it has deployed strong network defenses and must provide detailed records documenting every security event that the bank encounters, as well as the response. Although PVB's previous network security solutions provided an acceptable level of protection, the reporting capabilities were sorely lacking, making preparations for regulatory audits a time-consuming, cumbersome task.

[Find out how PVB shored up their reporting capabilities by downloading this whitepaper](#)

Leading Psychiatric Hospital Safeguards Key Healthcare Data

By Cisco and The Menninger Clinic

One of the world's premier psychiatric hospitals for over 80 years, The Menninger Clinic has earned a reputation as a leader in mental health treatment, research, and education. Information technology plays a vital role in supporting Menninger's state-of-the-art treatment programs. The network at its location in Houston serves 400 employees and spans seven buildings on 14 acres. Each building is connected via a fiber-optic backbone to a central server facility on campus that hosts information critical to treatment and hospital management.

Network integrity and security are essential to keeping Menninger's medical operations running. Like most healthcare organizations, Menninger must comply with the Health Insurance Portability and Accountability Act (HIPAA), which establishes stringent regulations for handling and safeguarding patient records. "Our biggest issue is HIPAA compliance," says Michael Farnum, information security manager at Menninger. "HIPAA requires that we document any network incidents and report them in a timely manner."

Menninger is a medium-sized psychiatric hospital with an IT staff of six. Manually tracking and reporting the dozens of network events that occurred each day made HIPAA compliance an increasing burden. "One of the main issues that I was confronting was simply checking logs and keeping track of all the day-to-day activity on our network," says Farnum. "I am the only dedicated security person, so it was a huge challenge." Farnum further commented, "We depend on our network and servers to support our patient information databases and our medication administration applications. We also depend on our network to document patient care on a daily basis."

[Find out how Michael improved network reporting to ease regulatory compliance and protect sensitive records with Cisco security solution by downloading this whitepaper](#)

Internet Content Provider Safeguards Customer Networks and Services

By Cisco and Synacor

Synacor used Cisco network infrastructure and security solutions to enhance network protection and streamline compliance. Fast-growing Internet businesses cannot afford network failures or security breaches. This is especially true for Synacor, a leading technology company that advances the delivery of meaningful content and technology solutions for multiple system operators (MSOs), telecommunication companies, and Internet service providers (ISPs) around the globe. Through Synacor's private label portals, subscribers can access a broad range of published and premium content, including entertainment, education, and family-oriented offerings from their homepages.

Today, through its service providers, Synacor's products and services reach more than 20 million broadband subscribers worldwide. With Synacor's business built around Internet products and services, network security is essential. The company must meet strict service uptime agreements and cannot afford to have its back-office assets or production networks disabled by a network attack. Additionally, as the company's business evolves, its security exposure has evolved as well.

"As we move to higher band-width media, movies, and especially gaming services, we are opening ourselves up to more threats," says Adam Howell, Director of Network Engineering and Systems Operations for Synacor. "One of our new accounts launching in 2007 will support more than one million subscribers right out of the gate and host a million e-mail accounts at our headquarters. We need to help ensure that there is no disruption or service degradation because of an attack on our network."

Synacor has heightened internal compliance standards. The company continues to be indirectly and directly involved in content sales, and with this enhanced activity maintains the protection of credit card information and complies with the Payment Card Industry (PCI) data security standard. As the company and systems grow and develop, Synacor's IT team is committed to making the technical infrastructure compliant with the U.S. Sarbanes-Oxley Act governing financial and accounting disclosure.

[Find out how Adam Howell, Director of Network Engineering and Systems Operations for Synacor did it by downloading this whitepaper](#)

Call for Participation

If you would like to be published in the Lippis Report, send your abstract to abstracts@lippis.com. If you would like to start a blog or author a podcast at the lippis.com site send e-mail to info@lippis.com.

Footnotes

If you would like to write for the Lippis Report, start a blog or author a podcast at the lippis.com site send e-mail to info@lippis.com.

Brief us on your new product or service to get featured in a Lippis Report Podcast. Send mail to briefings@lippis.com

Sponsor the Lippis Report and reach IT Business Decision Makers. Send mail to sales@lippis.com.

We are growing and hiring sales people. Please send resume to lippisreport@lippis.com

The Lippis Report is written by Nick Lippis, a world-renowned network architect and authority on corporate IP Communications. He consults to CIOs of Global 2000 companies and their direct staff on network architecture development.

You are receiving The Lippis Report email from us because you have either registered for an account on our website, registered for one of our webinars or conferences. To ensure that you continue to receive emails from us, add lippis@lippisreport.com to your address book today.

Please feel free to forward The Lippis Report to your peers. If you received The Lippis Report because it was forwarded to you, you are welcome to a free subscription at lippis.com.

Reporters are free to quote The Lippis Report with acknowledgement.

Notice: Equipment and service providers must obtain written permission to quote the Lippis Report in press releases, sales and marketing materials or to post, print or distribute any Lippis Report content in part or whole on any web site, print media or direct mail or e-mail distribution. A three month and unlimited license of the Lippis Report is available at sales@lippis.com

Entire contents © 2008 Lippis Enterprises, Inc. All rights reserved. Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Lippis Enterprises, Inc. disclaims all warranties as to the accuracy, completeness or adequacy of such information. Lippis Enterprises shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

[Privacy Policy](#)
