WHITEPAPER

Cyber House Rules

Empowering Visualization of Cybersecurity Information

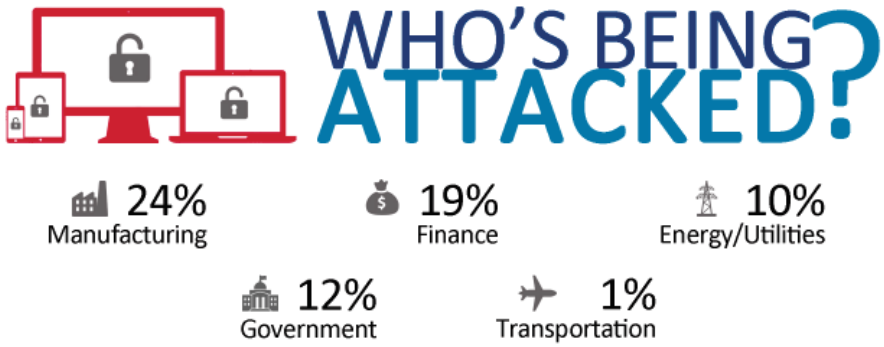
By John Stark, Vice President of Product Management
Activu Corporation

activu®

888-activu-1
www.activu.com

Recent well-publicized events such as the North Korean hack of Sony Corporation's file systems and email archives and the theft of millions of customer's sensitive data at Target, Home Depot and Morgan Stanley (to name just a small sample) have pushed cybersecurity to prominence in the public eye.

Although these events have caused many to question the safety of using modern financial and business systems, it is even more concerning that critical infrastructure – energy, transportation, and defense relies on the same technologies to enable effective communication and operations. A well-designed cyber attack on critical infrastructure could cripple a city, state, or even an entire sovereign nation.



Source: Internet Security Threat Report 2013: Volume 18, Symantec

Accordingly, many organizations are investing heavily in cyber security infrastructure, designed to repel unwanted intrusions, recognize suspect network behavior, and isolate viruses, spyware and other unwanted elements designed to capture sensitive data or cripple infrastructure. Often this results in NOCs taking on additional responsibilities in addition to management of IT services, placing more burden on already stretched resources.

The U.S. Government Reacts

Recognizing the importance of a governmental framework to combat cybercrime and cyberwarfare, the US government created the Cyber division of the Department of Homeland Security (DHS). From the DHS website:

> *"Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. A range of traditional crimes is now being perpetrated through cyberspace."*

Activu: Integral to Critical Operations

Central to the US effort to thwart cyber criminals and rogue nation-states, the DHS established the National Cybersecurity and Communications Integration Center to visualize, evaluate, and thwart cyber attacks on the US government and its critical civilian infrastructure. And when state-of-the-art control room collaboration and large scale visualization was needed, the DHS turned to the leader in network-centric control room visualization: Activu.

Vast amounts of visual information is generated through monitoring our nation's network, and sifting through that information is a daunting task. Activu Enterprise Software Suite enables effective visualization of key visual data and provides user-friendly mechanisms to manage and synthesize information into a common picture that allows cyberwarriors to recognize emergent threats and share that understanding efficiently; in the control room and across the agency, safely and securely, increasing the likelihood of detection and prevention of cybercriminal activity.

Activu Enterprise Software Suite: A Secure Network-Based Solution

Unlike a traditional AV solutions that offer security through isolation from the network and simply cannot provide the flexibility and reach that a true IT solution can provide, Activu Enterprise Software Suite was built from the ground up as a platform that would

integrate completely into an existing IT infrastructure, and by using state of the art development practices and security mechanisms, ensures its software meets the highest possible standards, allowing it to be used in the most security conscious environments in the world.

Standards Compliance

As the first visualization platform to be NERC-CIP and FIPS compliant, the AESS platform employs strong encryption for all its program communication, is delivered and deployed using a unique local virtual environment that ensures program integrity, and combines into existing user-level security environments (such as Active Directory) to ensure only authorized users are able to access information, and also provides additional tools to segment and apportion access to system visual information – giving administrators of an Activu system complete control over how, who and where information is distributed.

Coordinated Response: ActivShare

Instantly share critical visual information to ensure an effective coordinated response to a cyber event. Share one or more applications, screens, or entire desktops with multiple participants, securely and effortlessly. Collaborate with integrated chat and whiteboard. Share information to a common display wall in a network operation center, or simply make crisis meetings more effective by being able to share information in a meeting room or huddle space, instantly and dynamically.

Automated Visualization: Visual Intelligence

And to augment Activu's support of cyber security management, Activu Visual Intelligence can integrate with third party platforms (such as SNMP, email, etc.) and automatically visually alert users to nascent conditions that might otherwise be missed in the avalanche of information operators are asked to assimilate. Automated visualization can place content on specific users desktops or display walls.

About the Author

Drawing on over two decades of experience working with command and control visualization companies, John Stark oversees Activu's product management function, leading the direction and development of the company's future visualization, collaboration and mobility solutions for mission critical operations. Prior to this role, John has held research and development, product management and marketing positions with Christie Digital Systems, Jupiter Systems, Barco Visual Systems, M3i Systems and Matrox. He holds a degree in neurobiology and computer science from McGill University. He can be reached at 973.343.4956 or john.stark@activu.com.