

From: www.csoonline.com

Letters

CSO Contributor, CSO

October 01, 2003

IT's a Matter of Trust When waging war, it's important to know who your enemies are. It might be even more important to know the exact coordinates of your friends. But how can you trust those friends if you don't know how they operate? Our July "Hall Monitors" story emphasized the need to know who's on your network and how they operate.

Mapping networks and performing penetration testing may provide some confidence level, but if the people who we have holding the keys to the castle intend harm or to just plain rip us off, all the other work could be wasted. Strong, deep "people due diligence" should always be part of the mitigation plan. Many methods exist to accomplish this, such as a background investigation that could reveal a past history of similar behavior. It's the people, not the machines!

William M. Besse

Director of Corporate Security

Belo One Broken Window Begets Another Ever walk by a broken window in a rundown building and feel the temptation to throw a rock? Our June CSO Undercover column, "Broken Windows in the Boardroom," emphasized the importance of remembering the little things that need to be fixed. And to then dole out the accountability. This reader agreed.

Your June CSO Undercover article makes a compelling case for accountability as a fundamental tenet of risk management and security policy. Well done. It seems so obvious but, as the marketing executive for a startup who is building a tool squarely targeted at the "knowledgeable, empowered insider" from an information theft and misuse perspective, I've seen repeatedly the implementation of policy without the will or the means to ensure employees and other insiders are accountable and not merely responsible for their actions.

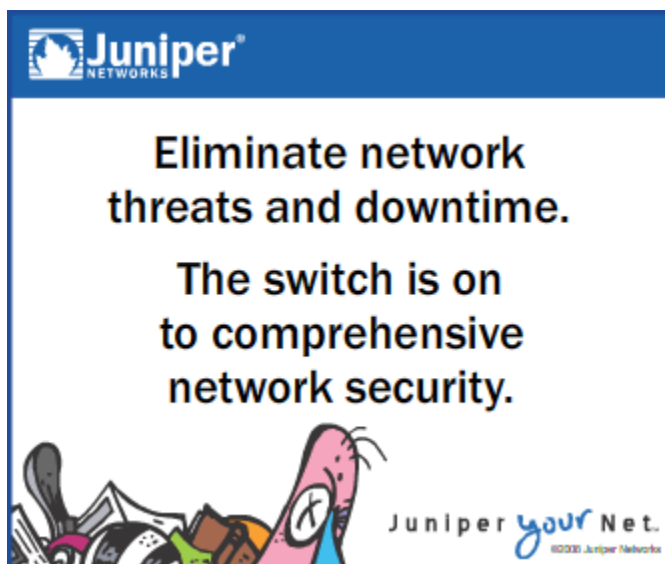
Bill Fletcher

VP of Business Development

Verdasys The Heat Is On In baseball, when a pitcher is described as "bringing the heat," it means he's going to throw the ball with great force. If you fear the heat, you'll need to step back from the plate. Same is true in security. But our July column, "If You Can't Stand the Heat, Don't Call 'Em," provoked a bit of rage. It's about calling in law enforcement the heat, if you will. Apparently, several of you won't.

This article unduly spreads fear and perpetuates the urban myth that calling in law enforcement for an IT penetration incident should be avoided. And it undermines our collective security efforts.

Calling in law enforcement when economic losses exceed \$5,000 (which is not very difficult to quantify) can



benefit a business by limiting liability, mitigating damage and helping stop perpetrators, yet it does remain a business decision.

Notification of the penetration through the InfraGard organization gives the company the choice to simply report without having company-identifying information revealed and allows others to be alerted to the exploit before they encounter it in their network on an opt-in basis. A simple report through InfraGard serves the higher purpose to reduce our shared risk. A critical mass of real-world incident data can contribute greatly to analysis and trending, resulting in improvements in preventive, investigative and incident-reduction efforts. Submission of incident data without fear of a confidentiality leak or loss of control is an important message and one that was completely missing in this article. For more on incident reporting through InfraGard, see www.infragard.net/ireporting.htm.

Betty Pierce
President
Secure Network Systems
FBI InfraGard Denver Board Member

A former security officer for the Department of Energy recommended a different route to report computer crime. I forwarded the process to a company that used it successfully. The company hired a private security company to come in and compile the evidence. The security company assisted in taking the evidence to the authorities. The process worked very well, and the company was successful in court.

Phil Shockley
CIO

Payday People Plus Patchy Prayers
In August, we told you to patch. And to pray. Some of you found that advice sinful.

Although patching is a chore, it is the only way to currently keep the vandals and their viruses at bay. Slammer was a very tricky exploit, but most worms are not as sophisticated and most patches are beneficial.

On the other hand, the big problem is the lack of liability that the software publisher faces in the real world. Every license stipulates that the publisher is not responsible for "collateral damage" resulting from the use of the software. This is like a carmaker saying that its liability is limited to the car itself and not the passengers or pedestrians.

If there is no incentive to make the software more secure through exhaustive testing, the publishers will not do it. If industry reviewers criticize a company for being late to market because of thorough testing, as Microsoft was with Windows 95, then we can expect more buggy code.

Software publishers have the most restrictive rights of any intellectual property I can think of. Along with that should come a responsibility to produce the best, most thoroughly tested product possible.

Terry Clark
Systems Manager
The Republic

We must find ways to automate the maintenance of systems. We cannot hope to defend against sophisticated automated exploits without sophisticated automated defenses!

Connie Sadler
IT Security Officer
Brown University

I want to specifically comment on the article's commentary that patching no longer works. There clearly are patch horror stories, as there are horror stories with every other type of security countermeasure. That doesn't mean that patching doesn't improve security as a whole.

While there is a need for improvements in the process of deploying patches, it does work when applied well. Do we claim that seatbelts don't work because an accident victim didn't wear one? Blaster was an example where well-applied patching greatly minimized potential damage; however, it was not a perfect solution. For that matter, nothing is the perfect solution. The only people selling perfect security solutions are fools or liars. What is needed


is Defense in Depth and properly trained staff. Articles that give the impression that patching as a whole is ineffective are dangerous.

Ira Winkler

Chief Security Strategist

HP

© CXO Media Inc.



**Eliminate network threats and downtime.
The switch is on to comprehensive network security.**

