



Getting the Bugs Out

By [Ralph C Jensen](#) Dec 01, 2009

When our publishers launched *Network-Centric Security* a few years ago, they looked at security over the network, how it applied to IP video surveillance and the quickly approaching revolution -- and called it convergence.

What they didn't take into account was how important the role of cyber security would play in the IP mixture. We aim to correct that today and in future issues of this magazine. Our editorial team will begin spending as much time researching the IT security side of integration as we spent reporting on convergence.

Convergence and integration are equals, and one can't succeed without the other. In other words, if the network isn't secure, convergence isn't secure.

"Today, digital images, seamless hybrid integration of analog and digital video, and automated retrieval of event information are commonplace," said Per Hanssen, president and founder of Salient Systems Corp. "The security and information technology worlds have progressed toward convergence, and IT support for video surveillance is steadily increasing. Management's demand for the collection, storage and rapid retrieval of video information is growing, and security managers are being required to provide regular reports to management on the integrity of the enterprise and to deliver analysis of threats captured on video."

The bottom line in convergence and integration is interoperability. Open standards will ensure that companies are able to choose the best product for their application. These applications include not only video surveillance but access control, building automation, command and control, situation management, visitor management and fire alarm systems.

Open standards are the key.

The IT security side is well aware of this concept, but it also has its challenges. Let's take, for instance, the emphasis on protecting insider threats. They can be malicious, but by the same token, they can be unintentional. Perhaps the most overlooked part of cyber security is that once someone has penetrated the network from the outside, they are now an insider. That means they can monitor very important inside activity.

Both roles of security are inextricably connected. They look at security in the same way but through different means. Security on the network means using best-of-breed equipment and having adequate bandwidth to process the flow of data, including enough storage space.

IT security faces similar challenges, but two of the most significant threats to corporate America are employees opening attachments in e-mails without paying attention to who is sending them. That's where most malware comes from. Another threat is social engineering. With seemingly credible e-mails from legitimate organizations, phishers can send bogus messages with malware attached.

These two resources are not on a oneway street; it's truly a two-way expressway for both sides of security.

“Both will be sharing resources and tools in the future,” Hanssen said. “From the physical perspective, they need the buy-in from IT, because they will be managing the resources. Physical security will become more logical because they need the expertise to protect it.

“IT security needs the physical side because it provides services, resources and tools to protect the logical assets.”

As convergence races forward, standards mean everything to security and security will mean everything to you and the end user as they work toward getting the bugs out.

About the Author

Ralph C. Jensen is editor-in-chief of Security Products magazine.

Copyright 2009, [1105 Media Inc.](#)