IT/AV REPORT
ADVANCING COLLABORATION & COMMUNICATION
VOLUME 13
NUMBER 2
Fall 2015

GREEN AVL AT HOOSIER ENERGY'S HQ

NEW LEED GOLD-CERTIFIED BUILDING WITH FUTURE-READY TECHNOLOGY.

Addressing The Skills Gap

Partnership strategies for the AV integrator.

How Secure Is Your Integrated Videoconference Room?

High-profile security breaches have exposed vulnerabilities.

Uniformity Leads To Change

University of Scranton upgrades and standardizes AV systems.

Signs Of Innovation

Digital signage serves up HD video with integrated, real-time ticket menu.

Viewpoint: Open Workspaces: What Are the Concerns?

How Secure Is Your Integrated Videoconference Room?

High-profile security breaches have exposed vulnerabilities.

By David Danto

For the past couple of decades, videoconferencing at large enterprises has looked pretty much the same. Yes, there was the Immersive Telepresence hype-bubble from 2008 to 2013 and, yes, there is always a drive to do more video from our desktops. However, for the most part, organizations needing to equip their facilities for videoconferencing went along the same path as they always did. Architects would design rooms, AV consultant firms would specify the components, AV integration firms would assemble the components and with any luck at all, the videoconference rooms would work.

Many have not realized it yet, but that model is no longer safe and will not continue. Systems designed with multiple discrete components that all have to ride on an IP network leave organizations vulnerable to malware attacks and security breaches. Recent high-profile security breaches and vulnerabilities such as Shellshock and Heartbleed have forever changed the landscape of videoconferencing's best practices.

VC Rooms Of Yesteryear

In the past, most of the room designs would look similar: There would be some sort of touchpanel that controlled all of the various components, some kind of flat-panel or projection displays, some audio speakers somewhere in the room, some microphones, a rack that holds all the components to make it work and, possibly, some cables and other input devices, such as PCs, DVDs, media players, tuners and the like. Most, if not all, of these components came from a different "best-in-breed" manufacturer.

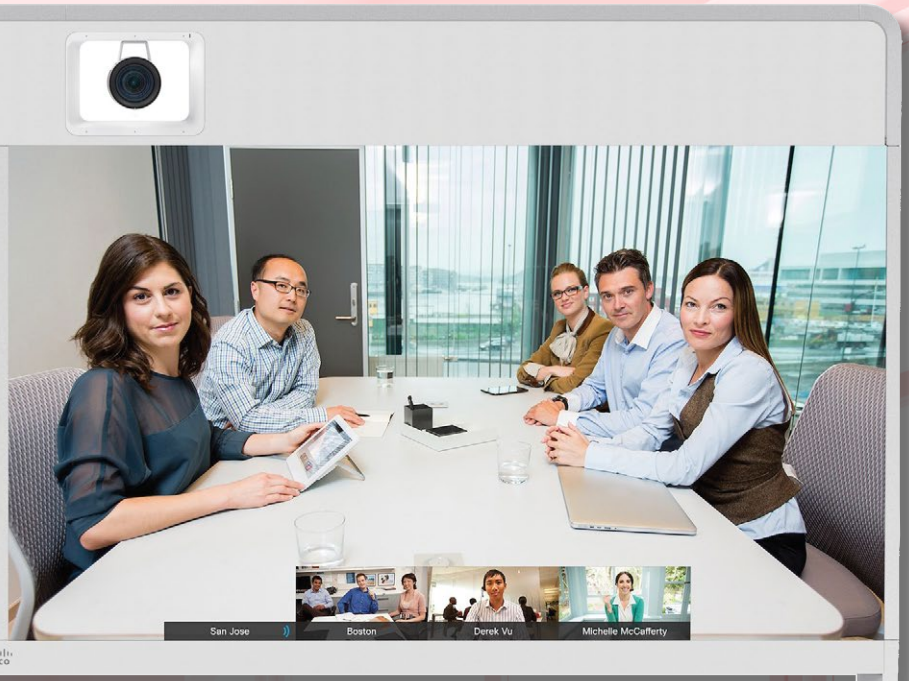
In some firms, these rooms worked well: Those typically had an internal or external management team making sure everything went smoothly. In some firms, the VC rooms worked poorly because end users were afraid of their complexity and no one was immediately available to help with reliability or operational issues.

Regardless of the performance experienced, the truth is, these rooms are now dinosaurs, and dangerous ones at that. This is because they are a security nightmare.

Network Security Issues

Over those same two decades, equipment manufacturers began to update their devices, requiring modern network connections to communicate with the other components in the room. Yes, the videoconference unit always needed a network (switched/dialed or dedicated), but now other devices, such as displays, processors,

David Danto is Principal Consultant at Dimension Data and IMCCA's Director of Emerging Technology.



Modern all-in-one systems are less vulnerable to security breaches, and can load any required security patches with little effort or risk of incompatibility.

cameras, control systems, audio systems and more, all have to ride on an IP network to operate. Although most people thought it was a good idea to modernize the connections, it regrettably opened up a huge bundle of issues around security.

One of my clients recently commissioned an analysis of the integrated AV and videoconference systems at its facility to determine how secure the systems actually were. The results were startling: 90% of the systems failed the most basic ITSM requirements. Issues were discovered in areas such as password handling, open ports, known compromised protocols, known vulnerabilities and more.

Even understanding which manufacturers provided support to fix new vulnerabilities was a daunting task. Some had the information and processes

The traditional integrated videoconference room with discrete components in a rack, all serviced by a technician's personal notebook.

New VC Best Practices

- No vendor-owned notebooks onsite anymore. Use the enterprise PC provided instead.
- Establish standard internal catalog.
- Favor all-in-one systems.
- Install updates in a rapid-response fashion.

Letting external service technicians connect their PCs to an enterprise network could be fatal.

detailed on their websites, some required a telephone call to their support hotline, and some provided no support at all. If one did identify a vulnerability and somehow managed to obtain and install a patch, it likely would cause the component to stop working properly with the others in the system.

Complex Systems

Keep in mind that these rooms typically have been so complex that they often required offsite "staging" and commissioning just to get them to work correctly in the first place. Making a change to one subsystem might require that commissioning to happen all over again, but this time as an unbudgeted expense.

The scariest discovery in the analysis was the realization that the standard procedure for adjusting or troubleshooting anything in the integrated system was to have an integrator's support technician come to the site and connect his or her personal notebook PC to the components. That external device, with none of an enterprise's standard security protections, could be the source of malware and viruses that could be transferred to a user's network via any one of the multiple components in the system. This is how one of the most infamous recent retail breaches occurred: A malware-infected service technician's notebook was connected to the firm's HVAC system.

Although a few enterprises try to mitigate the potential damage by isolating the AV system network from their core network in some way, there is no guarantee that components and/or users will not cross over at some point, enabling the spread of malware.

New Best Practices

What should organizations be doing to protect themselves from this threat? To begin with, I advise my clients to no longer permit integrators' notebooks to be used to set up or troubleshoot their AV systems. Each integrated AV system purchase should add the required service notebook to the BOM. This then becomes a typical enterprise PC running the organization's standard image, and is always connected to its network to ensure appropriate patching and protection. Should service work on an integrated system be required, the

external technician would check out the enterprise service PC and check it back in when the work is completed.

Honestly though, it's time to let the integrated videoconference room dinosaurs die out. A number of manufacturers now have excellent "all-in-one" room solutions for videoconferencing that mitigate most, if not all, of the security issues. When organizations choose these options, there is only one manufacturer to go to for security updates and patches; no update will disable other parts of the system because it's all a single product and, because the systems are the same at all user locations, one effort to research and patch resolves all open issues.

Internal Standards Catalog

If you have made the leap to modern videoconferencing systems, it is important to establish an internal "standards catalog" for your organization. This will list the types of rooms and systems that are acceptable for use within your organization. When a new vulnerability is publicized, the effort to patch all global systems becomes much easier if there is only a handful of identical system types in use at all of your organization's locations. All-in-one systems are again preferred because they are identical, regardless of the global region where they are installed or the installer used.

The frequency of new vulnerabilities also requires a change in how organizations approach updates. What was once a "take your time" process of lab testing new firmware and ensuring that it met all criteria before including it in an infrequent cycle, has been transformed by updates into a rapid-response requirement to squash vulnerabilities before they are exploited. Organizations need to have a skilled team rehearsed and ready to perform enterprise-wide updates at a moment's notice. This frequently tips the scales from an internal management team to an external managed service for videoconferencing endpoints.

So how secure is your integrated videoconference system? If it is more or less the same as it has been for the last couple of decades, that is, made up of multiple best-in-breed components, then, unfortunately, it's probably not secure at all. ITAV