by Tolga Sakman, Senior VP, Corporate Development and Strategy at Glowpoint

These past few weeks we saw a flurry of publicity around an Internet security consulting firm's findings on video conferencing and telepresence endpoints' vulnerability to hackers, as covered by articles in *The New York Times* and *Network World*. The sensational aspect was that someone – anyone – could potentially dial into your endpoint, and unbeknownst to you, could be watching you and listening to your conversations, zooming in and reading confidential papers left in a conference room.

Needless to say, the telepresence end user community took notice, and the video-centric blogosphere lit up with viewpoints that put varying degrees of the blame on the equipment vendors (they shipped the systems with the auto-answer feature on), the A/V integrators (they didn't setup a gatekeeper), the equipment installers (they simply don't understand security), or even the end users (just because they're always easy to blame).

I have been in the video industry for some time now, and the question of security comes up time and again. Let's clarify one thing: **the industry has developed and implemented high levels of encryption that satisfy the most security-conscious users, including the US Department of Defense** . So once a video call is on, it cannot be "phished" / listened in / watched, whether it's a point to point or multipoint call.

The type of potential security breach we are talking about here is mostly around systems set up with a public IP address, accessible via the Internet. In my experience, there are two reasons an endpoint might be deployed this way.

The first scenario usually occurs in a small firm with multiple offices of highly paid individuals, such as law firms and venture capital investors. These firms have typically deployed video after 2007 timeframe with the advent of HD, and have simply purchased 5-10 endpoints without any infrastructure, and have deployed them with public IP addresses with the intent of calling the other offices of the same firm. They mostly rely on embedded MCU capabilities of endpoints for multipoint calls.

In the second scenario, the main reason an endpoint has a public IP address is B2B (business to business) video calls. Typically, the vast majority of the video endpoints in the organization are behind a firewall and have private IP addresses, using a NAT (Network Address Translation) device, while a few select systems are given public IP addresses because the management wants to communicate with their partners / vendors / bankers / consultants / customers.

B2B Video: Is it a pipe dream?

For a number of reasons, the overwhelming majority of video calls today are intra-company, although it's been technically possible to traverse firewalls and NAT devices for some time now. The problem is two parts interoperability challenges between different vendors' equipment (yes, I know, we are still dealing with this issue in the year of 2012), one part lack of network peering (you're on AT&T, I'm on Verizon, the rest is history), and a large scoop of lack of a universal dial plan.

Read that phrase again – lack of a universal dial plan. Think about it: you have video in your organization; so does your customer. You use 4 digit extensions to dial others in your organization, but your customer's business card shows a video number with 5 digits. How do you "dial 9 to get out"? And then what?

When you look at our industry from this perspective, it really resembles the infancy of the telephony industry over a century ago: organizations deploy video internally and then an "operator" connects them to the outside world if and when they need to make intercompany calls. It's cumbersome at best, and definitely not in sync with the ad hoc nature of our work environment today.

So enterprises go for the easy fix – put an absolute minimum number of endpoints up on the public Internet, so that they're reachable via IP address dialing. Regardless of the auto-answer feature being on or off, this is not the most elegant solution. It creates unnecessary vulnerabilities and generates silos within the silos of already isolated video islands.

Following the telephony example of over a century ago, the ultimate solution to the B2B problem that will succeed is **a cloud-based registry system that creates a universal dial plan and opt-in directories** .

At Glowpoint, we are putting together exactly that: a B2B Exchange platform within OpenVideo cloud that provides a universal video number to all registered systems, with the end goal of enabling ad hoc, direct dialing outside of the enterprise. Much like your PBX-based desk phone having a 4 or 5 digit extension that can be dialed internally, while also having a 10 digit number (using US as an example) that can be dialed from the outside, your video endpoints will remain registered to your in-house gatekeeper / SIP registrar (if you have one), while also having a universal number that can be dialed from "the outside."

Going back to the scenario #1 above, where endpoints are exposed to the Internet due to lack of in-house infrastructure, OpenVideo is also your cloud-based call control. You get connected, get a DID (direct inward dialing) number and live grand, making seamless B2B calls, using the directory.

Security or B2B? You need not compromise; you can have them both!

Despite the average prices coming down, video is not a cheap technology.

You have invested a lot of money into your video deployment. There is no reason it should be limited only to calls between your offices. The more you can visually collaborate with your customers, partners and vendors, the more value you will get out of your investment. But you should not see the equation as one of compromise between B2B and security.

Using a cloud-based B2B Exchange service such as what we have in OpenVideo, you can B2B-enable your entire video estate with the peace of mind that it remains secure and behind your corporate firewalls.

Glowpoint runs the largest B2B Exchange in the world by number of systems, and has strategic partnerships with major providers and carriers in this space that makes it an integral part of this “cloud of video exchange clouds.”

You have already invested in video, because you believe in its power. I say unleash its potential by enabling seamless, secure B2B connectivity in the cloud.

Tolga Sakman *is the Senior VP, Corporate Development and Strategy at* ***Glowpoint****. Glowpoint provides cloud managed video services “that make delivery of consistently high-quality video conferencing and telepresence service as simple as the Internet, between any endpoint, network and business.” Tolga joined*
Glowpoint
in 2011 and is responsible for Corporate Development initiatives and overall corporate strategy. He has more than 15 years of experience in directing corporate development and M&A initiatives, strategic alliances, market research and competitive intelligence operations, industry and financial analyst relations, strategic and financial planning and analysis for global enterprises.

*Prior to joining Glowpoint, Tolga was with the **TelePresence Technology Group of Cisco**, working on Market Development initiatives. He joined Cisco through the*
TANDBERG
acquisition, and was instrumental in setting the regulatory approval strategy for the Cisco/TANDBERG deal. He is considered an expert in Unified Communications, Video Conferencing and Telepresence industries, participants and the underlying technologies.

*Tolga earned his MBA in Strategy and Entrepreneurial Finance from **Penn State University**, his M.Sc. in Engineering from*
University of Cincinnati
and his B.Sc. in Engineering from
Orta Dogu Teknik Universitesi
in Turkey.

Go Glowpoint Blog