Beyond the Network: Skeletons in Your Data Closet

There are problems lurking in networking and computer rooms around the world. Messy data cabling, discarded litter or random junk that simply shouldn't be in a space for communication equipment. Having such skeletons in a data closet can make a business vulnerable to accidental downtime, reduce employee productivity and in extreme cases even pose a safety hazard.

One company is using a surprisingly simple mix of plug-and-play technology and good operational processes to ensure that thousands of these often-overlooked spaces get the oversight they deserve. Doug Alger unlocks the secret to banishing skeletons from data closets as we go beyond the nework with Cisco IT.

DOUGLAS ALGER: "Habit is a cable; we weave a thread of it each day and at last we cannot break it. Horace Mann, American education reformer. Horace passed away in 1859, so he obviously wasn't talking about a modern data closet, and yet... anyone who has ever worked in or around networking rooms has likely encountered bad habits and crazy cabling at some point.

I spoke recently with David Laban from Cisco IT. He's based at the company's UK office and has been working on an initiative that improves how such spaces are managed.

DAVID LABAN: "So, I'm a network engineer within Network Services. Now, the role of network engineer can cover many things and I primarily focus on network design and acquisition implementation. So I basically do a network design and speak to customers and stakeholders and get a real feel of what their requirements are and then put together a network solution which maps to something we have within Cisco IT, particularly within Network Services. And actually go there for those acquired sites and deploy that solution.

DOUG: "His team has just completed a pilot project, deploying about 120 cloud-managed Meraki cameras into rooms on three Cisco campuses – one in Bangalore, India, another in the London Heathrow area, and the third at Cisco headquarters in San Jose, California. They're preparing to roll the project out at scale, ultimately deploying thousands of cameras at about 500 offices worldwide.

We talked about some of the surprises to be found in these rooms – what I call wiring closets and David calls comms rooms – the challenges they encountered, and how they expect to readily monitor and manage thousands of these environments going forward. We began by talking about why they took on this task."

DAVID: "Comms room consistency and comms room cleanliness is a, say, bit of a problem – or has grown to be a bit of a problem over the years. And by problem I mean cabling standards and then also the fact that people are using the rooms for things that the rooms shouldn't be used for. So first of all in terms of cabling standards there's some cables that may have not been patched the correct way, or cables that have been run over the top – they're not following the best practices, so sometimes you can get what is known as a cable jungle, whereby the front faceplate of a rack in a comms room is just completely covered by fiber and copper. That's something that this project looks to address by the fact that we actually put cameras in comms rooms and monitor the room and standards. The other area that I mentioned was there's an issue with people using the comms room for storage. Some people have even put their bicycles in the comms room and stored those. Some people have put boxes in the room that shouldn't be there. Or people have installed some equipment and then not taken the box out of the room, so having these cameras in those rooms is going to allow us to actually one, ensure we know who is in the room and then, two, highlight any issues that we may need to actually address by – if we see there's actually a bicycle or a box that we would send somebody local there to remove that box and make sure the person that is doing that isn't repetively offending, if you will."

DOUG: "I have to say, I started off in IT doing a lot of work in Data Centers. One of the first projects I was ever involved with was stocking patch cords into wiring closets across Cisco's main campus – I believe they had about 150 different rooms. Over the years I've had a chance to go on a lot of different Data Center networking room tours. I actually wrote a book on interesting Data Center projects, so I've seen rooms that look pristine and they're very well organized and they're color-coded and everything is beautiful… and then I've seen the other end of the spectrum. You mentioned bicycles. I've seen weight room equipment. I've seen a lot of strange items that show up in these rooms. What were some of the oddest things that you've come upon over the years in these spaces?"

DAVID: "So some of the strange things that we've seen as well – we've mentioned that there's bicycles and you've mentioned that there's weight equipment – and that's crazy. Some things that we've seen is, like, network equipment that's actually been hanging from the ceiling. It was actually in a site in Hawaii so it's kind of fitting that we said that the equipment was sort of surfing off the ceiling. Obviously that sort of thing is something that we want to ensure never happens, so that's why having these cameras in these rooms will help us detect and prevent any of these issues happening again."

DOUG: "There's obviously the what-were-people-thinking aspect when you go into some of these spaces. But this is important for a business reason, to be keeping track of what's going on in these rooms, yes?"

DAVID: "Yes, absolutely. So, I mean, what we've been speaking about here is mostly cleanliness but obviously cleanliness drives safety and therefore when you have safety you can prevent any accidents or issues happening in the room. And some issues, accidents, could be like, if someone's bringing a bicycle or weight equipment into a room and that equipment snags on a cable that could then therefore cause an outage, which is going to be monetary, revenue impacting to the business. So, yes we were talking about keeping the room clean but the direct reason why is so that the only things that should be in these comms rooms are things that are related to comms. So, networking equipment and then cabling. So when we monitor and ensure the standards of these rooms that's how we can ensure that we have the maximum resiliency and protection for any issues that may occur on a physical layer in the room."

DOUG: "What's the biggest challenge to doing this?"

DAVID: "Well, simply, the biggest challenge to doing this is the fact of how many cameras we're going to have to put out there. Throughout Cisco we have over 500 offices. Within that some buildings can have four, maybe even six or eight, different comms rooms within them. And when you put a camera in every row of every comms room – so if you were to do the numbers, that can be over 10,000 cameras. We're starting at the largest campus sites so some of the challenges that we're having are just getting the cameras in because there's so many to do. So it's about having a deployment schedule and actually getting the project off the ground and getting the resources and the workers to actually go and deploy these cameras."

DOUG: "When this is complete will there be more than 10,000 cameras deployed in these different spaces?"

DAVID: "Yes, and I've done the quick math and it really depends on if we want to target every single comms room of every single site or if we want to target the most critical ones. This project is very much in the beginning stages whereby we just reached global deployment – GD status – which means that the three pilot sites that we've completed – those have just completed their pilot phase and now we're going to GD status which means we're actually rolling these out as part of fleet cycle. Meaning that when we actually deploy buildings the cameras will do into the BOM, which is the Bill of Materials. So as we're rolling out sites this will be happening. So to answer your question, yes, I do anticipate over 10,000 cameras being deployed. The exact number will be more known as we get deeper into the deployment schedule."

DOUG: **“**How long is that expected to take?”

DAVID: **“**A fleet cycle for any one given building, a building becomes eligible for fleet after three years, so that’s not necessarily meaning that we’re going to upgrade every building after three years but you can anticipate that if it was on a rolling schedule there would be more and more happening after the three year point. Obviously some sites are up for fleet now but we’ll be into a full cycle of deployment after three years.”

DOUG: **“**So let’s look ahead to that. When you have thousands of cameras deployed, how do you keep track of it all?”

DAVID: **“**So, we use Meraki Dashboard for monitoring these cameras, and Cisco IT has a great partnership with Meraki IT and we cooperate with many different initiatives and this particular initiative we are utilizing the camera technology. So we have a camera network on Meraki Dashboard and that’s where all of our cameras are added to and monitored from. The best way that we are tracking these cameras is creating video walls so you actually can see a view of a whole floor worth of cameras or a particular site and then you have various tabs along the top of the video wall so that you can switch context and switch building. So you don’t have to individually click into each camera to be able see the footage. You can see it from a more high level view of that building or that floor or even a combination of multiple floors if you have enough cameras that are covering those two floors.”

DOUG: **“**So the picture I have in my mind is one person, in front of a very large bank of screens and they’re trying to check every single one. I have a feeling that wouldn’t scale very well.”

DAVID: **“**Oh, no. So Meraki Dashboard is where a person goes to to check but it’s not going to be one person that’s monitoring all these cameras. We have camera operators globally dispersed that are tasked with monitoring the camera feeds and checking for any issues that are occuring. So we have, on that point, monitoring. There are people that are monitoring the cameras in the global regions – because we operate a follow the sun model within Network Services – and then in addition we also can respond to alerts or triggers or somebody says ‘Hey, I’ve just been in the room and I found this.’ We actually then can go onto that site, look at the camera and as you know the camera technology has an SD card inside of them. So these MV21 Cameras have a 128 Gigabyte internal SD storage. We actually can go back in time and look as to when the event occurred, so they’re not a live feed camera in the traditional sense. They actually have the live feed cameras as well as going back in time to look at any historical events that may have occurred.”

DOUG: **“**So from what’s been deployed already, have their been any surprises – aside from crazy things that may have been found? Any lessons learned for how you approach this?”

DAVID: **“**Yes. So, from that statement, we have 119 cameras deployed and since deploying them we actually saw that in one of the comms rooms the room got kind of hot and the solution was somebody propped open the door. Clearly that’s a violation of policy and the camera alerted us to that immediately so that we made sure the door got closed. That’s just some of the things that we’ve seen. I’m probably sure there’s a few others. It’s not just me monitoring those cameras so I’m sure that others would have other stories.”

DOUG: **“**With the cameras in place, when you discover that a door has been propped or you now have visibility into the way the cabling is – good or bad – when you encounter a problem what then happens?”

DAVID: **“**When we encounter an issue we’re obviously drawn to the fact that there’s a problem. We can do one of a few things. If there is somebody in our team who is actually local to the site then we can actually just go there and address it ourselves. But if we need to engage some other local IT or some other assistance that’s outside of our group then we can raise that local support case to have somebody go there remediate the issue. Our team is dispersed around the world so more often than not we have the capability of addressing these issues ourselves. And from what we’ve been finding these issues are happening are more of the larger campus sites where we definitely have Network Services presence at.”

DOUG: **“**Is your sense that when you find strange things in these spaces or something has been miscabled – does there tend to be a particular reason why? Is this a case of there aren’t rules in place for it? Is it because there’s a special set of circumstances that are causing this to happen? From what you’ve been ability to see, the visibility that you’ve been able to get so far, are there any patterns you’ve picked up on?”

DAVID: **“**It’s important to note that we have a set list of best practices that we give to our vendors and employees for when they go into comms rooms and perform cabling work. Sometimes the case happens whereby these best practices aren’t followed and sometimes we simply don’t know whether it’s our vendors or which vendor or if it’s somebody or a team internal, Cisco employees. So this camera technology gives us that capability of identifying which group is potentially violating these rules. And it could be because they simply don’t know what the rules are. Maybe they didn’t actually read the document that we gave them. So this technology allows us to identify people or groups that may need to have refreshing on what the policy is and that camera technology allows us to identify who that is so that we can engage with them and aske them, firstly, why did this happen and then, secondly, go fix it.”

DOUG: **“**So I’m sure there are a lot of people out there listening that have wiring closets that are not pristine. Any recommendations that you would have for them – if they’re trying to get a handle on what’s happening in those spaces, any general advice you would offer?”

DAVID: **“**The first piece of advice is to make sure the room itself, the comms room, is badge access controlled so that you have at least some control on who is going into that room. Then secondly you want to make sure that people in that comms room who do have the access are following some type of best practice or standards that have been written either by the company or by industry standards, because there are cable industry standards that are out there for you and I to read and there are IEEE standards for best cable practices. Then once they’ve got room in the standard they want it they want to keep it that way, so they could leverage a solution like ours by putting these cameras in each of the rows in that comms room. They can make sure that the standards they’ve set and worked so hard to uphold remain that way. So that’s my advice to them. Get it clean and then get the cameras in.”

DOUG: **“**And then in terms of scale – not everyone necessarily has 10,000 spaces that they’re trying to keep track of, but they may still have a significant number and this can probably seem pretty daunting to try and get this deployed in mulitple locations. Any good recommendations on how to approach it?”

DAVID: **“**A lot of the areas that have the high footfall and that have a lot of people coming into those comms rooms are those campus locations so I would start with the HQ and then work out to the branches because typically the locations that have the most amount of traffic in terms of people going through the office – not network traffic – would be more susceptible to these types of issues. So my advice to them is to start with the HQ.”

DOUG: **“**What’s the definition of success for this project?”

DAVID: **“**The way that we’re going to measure success of this project is that, ideally, we should not be finding any more issues or any more things going on in the comms room. The cameras themselves act as a deterrent in their own nature to stop people coming in and doing things that they shouldn’t be because as part of this camera deployment we have to comply with Cisco’s internal legal practices, we have to put a notice on the back of the door for people in the room to know that yes the work that you’re doing in this room is monitored for cabling standards and best practices. So, ideally the objective is that we don’t need these cameras any more because they would just be looking at perfect, pristine clean rows.”

DAVID: **“**As this project progresses further into its maturity then we also could look at abstracting metrics on how much cost it saved the business by risk reduction in terms of preventing outages that would have happened in the comms room from people cabling in an incorrect standard or storing things in the room.”

DOUG: **“**Were there any surprises that bubbled up during the pilot?”

DAVID: **“**One of the surprising things that we found about this solution was actually how simple it was really to do. The cameras themselves, as soon as you plug them in they – as soon as they can get a DHCP address – then they just sync right into the dashboard so there’s like no configuration at all that’s required to do on the cameras. So that was pleasantly surprising if you will. So yeah, that was a nice surprise for us.”

“For those that are interested, the camera model that we’re using is the Meraki MV21, which features 128 GB internal SD storage, and this camera is cloud-managed so you just claim the serial number from the camera on Meraki Dashboard and that’s how you manage and configure the device. All configuration is done on Meraki Dashboard and the camera pulls down the configuration from the cloud. So you can setup your camera deployments prior to the equipment even being shipped to the site and as soon as that camera has an Internet connection then it will sync to Meraki Cloud, pull down the configuration and you can view the footage on the Meraki Cloud, meaning you can stream directly from the camera to your web browser and you can also store – if you want additional storage than the 128 GB SD card – you can leverage AWS to actually ship off that data into AWS Cloud Storage solution that Meraki has partnered with.”

DOUG: **“**Aside from the scale, this actually sounds like it’s reasonably straightforward to get these installed, to get them up and running and then be able to do this monitoring. It really sounds for as large as a project as this is, a lot of the steps along the way are going to be pretty simple.”

DAVID: **“**The solution itself is very simplistic in nature. The difficulty comes from doing it at the scale that Cisco IT is. And as I mentioned, we’ve just completed the pilot phase. We now have to do a transfer of information whereby we’re writing technical guides, and implementation steps that will go to our vendors who actually will be doing the implementation from there on out for our global deployment.”

You’ve gone Beyond the Network, with Cisco IT. Thanks to Sarah Khokhar for recording assistance. This episode was produced by Douglas Alger. Follow and like our podcast on SoundCloud or iTunes.
Visit cisco.com/go/ciscoit for episode transcripts and related content.

For More Information

To hear additional Beyond the Network podcasts visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit.

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.