After Cyberattack, a CEO Speaks Out

Exhaustion, dark-web threats and lingering trauma: Colt Technology CEO **KERI GILDER** on the toll a breach takes on employees and leaders. By **NICOLA HUDSON**

On August 12, 2025, a cyberattack was launched on Colt Technology Services, a privately owned London-based global telecommunications and network provider. The attack disrupted the company's internal business support system, leaving existing customers largely unaffected, but limiting Colt's ability to develop new contracts, among other challenges.

Colt took instant action to isolate systems and contain the threat. While systems were restored, to CEO Keri Gilder the incident is anything but forgotten. And she doesn't share the widespread disinclination among CEOs (and their lawyers) to talk openly about the experience of being targeted by cyber criminals. Gilder sees the sharing of information as a crucial element of disaster preparedness.

Conversely, Gilder believes staying quiet may actually benefit bad actors. "Transparency was always our policy, and why would we change that now?" she asks.

A former network engineer, Gilder worked for 16 years at Ciena before joining Colt in 2018 as Chief Commercial Officer. Since becoming CEO in 2020, Gilder has become a prominent industry voice on digital infrastructure, connectivity, and inclusion and diversity. What follows is an edited conversation between Gilder and Brunswick Partner Nicola Hudson OBE, former Director of Policy and Communications at the UK's National Cyber Security Centre, and former Head of Communications at the UK Prime Minister's Office. Hudson has worked on hundreds of cyber security incidents, including having served as a communications advisor to Colt.

Could you take us back to August 12, 2025, when you first heard about the cyberattack?

I was seven time zones away on a different continent, and it was around two in the morning that I was notified of an imminent Gold call [Gold refers to Colt's executive crisis committee]. This wasn't unusual. Because we have fiber cuts from time to time, we're kind of used to being called in the middle of the night. My first reaction was, "Whatever it is, we'll get through it."

But then, ahead of the call, my Chief Information Officer called me and said, "This isn't a normal fiber break; it's a cyber incident." He told me we'd already shut down a number of servers. That call came two minutes before the Gold call, and thank goodness. Now I understood the gravity, and I knew I had to be calm in order to set the tone for the Gold team.

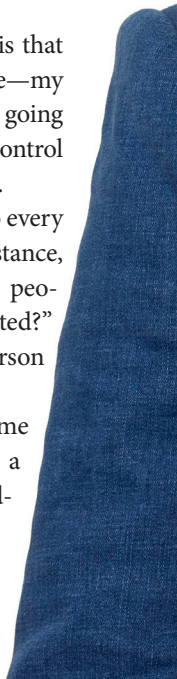
When I got on the call, the Gold team was hearing about it for the first time, and what I saw was shock. I could see a fight-or-flight response across my leadership team. I'd planned to say, "What are the next steps?" But I saw that this was not the moment to start rolling out actions. They needed a few minutes to absorb this.

"We all have the same information now," I told them. "So we're going to leave this call and jump back on in 15 minutes. I want you to think about how this cyber incident impacts your function, your area and what we need to do next."

What I realized during those 15 minutes is that my normally collaborative leadership style—my preference for decision by consensus—wasn't going to work here. This needed a command-and-control approach, which was a way I'd never operated.

During those 15 minutes, I sent an email to every single one of my direct reports saying, for instance, "You're head of HR. Please think about the people ramifications. How are our people impacted?" I did that with every single executive and person who was on the Gold call.

I told them what to do, and when we came back on the call 15 minutes later, there was a greater sense of calm and a better understanding of what each of us needed to do.



"THERE'S A LESSON: WHEN YOU RECOGNIZE A GAP, ACT QUICKLY TO FILL IT. YOU HAVE NO IDEA HOW SOON YOU MIGHT NEED THE FIX."

You make an excellent point; in a crisis you often have to dictate what needs to happen, and when, rather than seek collaboration as usual. Also, the fact that the CIO called you before the Gold call shows that you had a relationship with the CIO, who at many companies has no seat at the executive table. To what extent did you have a playbook for this type of crisis?

We had done half-day practice sessions where we would bring in an outside partner and run through a crisis scenario. In this case, it was fortunate that we had just held one of those sessions about a month before this happened. We take that kind of training seriously; we treat the crisis as if it is actually happening. Every single time, we pull up our Business Continuity and Disaster Recovery plan and augment it with our new learnings.



That training we underwent just before the cyberattack was around a hypothetical crisis that was social in nature—sexual harassment, for instance. And that session made us realize we had no real crisis communications capability for anything that wasn't a telecommunications issue like a fiber cut. That realization led us to put a contract in place with Brunswick for crisis communications management, should it become necessary. We had no idea how fast it would become necessary.

In that case, we acted on what we learned from the exercise as soon as we saw the gap, which frankly we hadn't always done. There's a lesson: When you recognize a gap, act quickly to fill it. You have no idea how soon you might need the fix.

Of particular importance is that we had created a decision matrix: If a particular thing happens, who is authorized to make a decision? In the case of a cyberattack, authority belongs to the head of cyber. And that's who shut down a number of servers before I even knew there'd been an incident.

That suggests you'd built a lot of trust in the process and your people. I've worked with organizations where a particular team was empowered to act but didn't do it. To make that decision is hard, right?

The person who made that decision wasn't in the executive leadership team. Nor was he a director. Yet at the CIO's suggestion he came on to that Gold call during the first hours of the crisis, and he was nervous, even though it was written down that he was empowered to take that decision. I had to reassure him and everyone else on that call that he had done the right thing, and I thanked him for protecting the business. It was important to give him and anyone else who needed it a sense of psychological safety. People will avoid difficult decisions if they're worried about getting fired.

I've seen cases where the authority for front-line people to act was written down, codified and still they were too scared to do it. What was the most surprising challenge you faced?

When it happens to another company you don't necessarily appreciate how mentally and emotionally and physically devastating these attacks can be.

Three weeks into the event, three weeks of working pretty much 24/7, I was exhausted, totally lacking in energy, and I realized that an element of self-care needed to come into play. So I made sure I wasn't over-caffeinating, made sure I was drinking plenty of water and eating healthy food, not a bunch of

sugary foods. Most importantly, I started trying to get more sleep and go for walks. Taking walks, getting fresh air and experiencing nature—those things became extremely important, especially given the unrelenting attacks on the company and me.

You personally?

I started taking walks at 6 a.m. with my husband. He's a good listener. One morning I was just talking through what was going on when I received a text from my CIO. He passed along to me something he thought I should see, something from the dark web. It was basically an attack on me. It said, "If you're a customer of this CEO, I recommend walking away. If you're an employee of this CEO, why would you want to work for her?"

That was probably my darkest moment. My resilience was a bit low, and I started doubting myself. "Am I doing the right thing?" I wondered. I was following the guidance of various partners around me, but how could I know? I'd never handled a problem like this before. Luckily, my husband was right there. He said, "What are you talking about? These could be teenagers. These could be people involved in the attack. They're trying to get to you psychologically. Don't let them." And that helped build back my confidence. It also impressed upon me the importance of having a confidant, because you can get too tired to see or think clearly.

After that, during a Gold meeting, I asked every single person on the call, "Who is your confidant? Personal or professional, who is your confidant?" What I found fascinating was that the people who were thriving had both professional and personal confidants. Those who were not getting through it well lacked one or the other.

Any other advice for a CEO about how best to prepare or respond?

One, educate yourself about cybersecurity, even if you think you already have. Every CEO should read the Cybersecurity Framework from the US National Institute of Standards and Technology.

Two, fix forward rather than blame backward. Many people in the organization were thinking, "Did I click on a link? Was it me who actually caused this?" Within the first few days I got on a call and I said, "This happened to us. It didn't happen by us. Nobody is to blame here." Sure, we're going to investigate how it happened, for legal purposes and to make sure it doesn't happen again. Every week we held company-wide calls, and at every meeting I said, "We're fixing forward, not blaming back."

"EVERY WEEK WE HELD COMPANY-WIDE CALLS, AND AT EVERY MEETING I SAID, 'WE'RE FIXING FORWARD, NOT BLAMING BACK.'"

Three, stick to your values, personal and corporate. From the start, we were committed to transparency, with customers, employees and everyone else. At times, outside counsel advised us not to talk about certain things. And honestly, not talking about it was probably the less risky strategy. But that didn't feel right to me. We're a private company, so maybe transparency is a little easier for us. But we chose to release all the information that we could to our employees and our customers. And it made them feel as though this was the Colt they'd dealt with forever. Because we were transparent, I believe we may have avoided some future legal issues.

How did you guide your global staff through this?

We went 16 weeks before our critical people had a weekend off. During that time, we kept them close, supported them, advised them to prioritize their welfare. We had conversations about using mindfulness and breathing techniques for those who found that helpful. But we were still pushing our critical teams 24/7 because we were losing business.

Then one of my confidants—someone at a different company who'd been through a trial like this—told me about the personal physical toll it took. That woke me up. On the next Gold call, I said, "Guys, we need a time-out. These people need a weekend off. I understand it's going to delay us. I understand we may not hit our deadlines." Better not to hit those deadlines than to have your people in the hospital. Beforehand, that idea could not have been more foreign to me.

There were also people in distress because they had nothing to do. Their systems had been shut down. All they could do was think about the impact on them, on their customers, on the business. Some of them went into a dark place. They were asking, "What can I do?" So I worked with our HR team to find ways to make them feel productive. We moved a lot of our sales people into communications, for instance.

The last thing I'll say is that post-traumatic stress can strike after an incident like this. The most critical people will be in overdrive during the most intense part of it. You'll see people missing work because of stress or high anxiety. You'll see people with some health issues; no human being is necessarily immune to that. You've been attacked, and the human reaction to being attacked persists well after the event is over. As CEO, you have to pick up on these signs, recognize the strain it has on everyone and act. ◆

NICOLA HUDSON is a Brunswick Partner with deep expertise in cybersecurity issues and crisis management. She is based in the firm's London office.