

Customer Experience Leaders Must Step Up to the Cybersecurity Challenge


By: Connie Moore

An Interview with a Cybersecurity Expert

This research brief is a transcript of an [interview](#) between Connie Moore, Vice President, Research, at Digital Clarity Group, and Juanita Koilpillai, CEO and founder of Waverley Labs, a cybersecurity software and services company. Ms. Koilpillai is also one of the co-founders of the Digital Risk Management (DRM) Institute, a nonprofit organization established to expand the dialogue and knowledge about cybersecurity by helping business and technology leaders realistically determine what types of cybersecurity risks they face and what can be done about them.

The interview focused on two nascent but important trends for 2017:

- **Cybersecurity collaboration.** In forward-looking companies, the chief risk officers (CROs), chief security officers (CSOs), and chief information officers (CIOs) will begin in 2017 to collaborate not only with each other, but also with chief marketing officers (CMOs) by including them in discussions about how to mitigate [cybersecurity risks](#) that could seriously deteriorate customer trust.¹
- **Software defined perimeter (SDP).** A small but important number of large organizations will begin shifting from fixed cybersecurity architectures to a safer and more flexible approach known as the [software defined perimeter](#). This approach is more secure because it is significantly more closed to intruders than architectures currently in use, but it needs to be considered carefully. The tighter security measures that safeguard customer information could also make it more difficult for customers to engage and interact with those firms. Finding the balance will be important.²



Moore (CM): *Welcome, Juanita. I'm thrilled to have an opportunity to discuss with you how cybersecurity impacts the marketing organization and to examine how the software defined perimeter improves cybersecurity measures in business and government agencies. These are vitally important issues.*

Koillpillai (JK): Thank you, Connie, for this opportunity to speak with you. It's great that you and Digital Clarity Group are focusing on this topic from the unique perspective of customer experience leaders.

CM: *I can just imagine that CMOs and customer experience leaders may be curious and perplexed as to why we are tackling this subject, because it may seem so far afield from their usual focus.*

I recently attended a digital marketing conference where everyone was a director, VP, or CMO. While there, I talked with some attendees who worked for companies that had experienced breaches. I asked a few of them to what extent and how effectively the marketing staff was working with risk and security people. Most of them looked at me blankly and said, "We're not."

But I think cybersecurity, customer privacy, and trust are interconnected subjects that should and will soon matter to marketing organizations. Plus this topic is quickly moving from "below the radar" to high visibility as Europe readies to launch the [GDPR legislation](#) on May 25, 2018.³


Juanita, what connection do you see between these two topics? Do you run into collaboration or compartmentalization with the companies you are working with?

JK: It's still very nascent for these different disciplines to work together at the executive level. It was only in 2016 when executive boards got involved in looking at cybersecurity. That largely happened when people were fired over breaches in some organizations. More business and technology leaders are now at least trying to have the conversation about how cybersecurity impacts the entire enterprise. Up until now, it has been the CIOs bubbling this topic up to the C-suite, so it's a new conversation across the leadership in most organizations. At the Digital Risk Management Institute we are trying to help foster that conversation and shape what it should look like.

CM: *How is cybersecurity related to CMOs? They are probably saying, "Gee, what does this have to do with me or my company or what I do on a day-to-day basis?"*

JK: CMOs have a huge stake in whether their companies are hacked, because it exposes highly confidential data [such as sensitive medical information or private financial data]. This information has a huge exposure. The elevation of cyber to the C-suite will force the CMO to be a player in how the organization proceeds. This is one of the emerging trends for 2017 and beyond. It's just like how social media changed the way

... cybersecurity, customer privacy, and trust are interconnected subjects that should and will soon matter to marketing organizations.



CMOs approach their jobs. Elevating cyber is going to change the paradigm from a security/risk/technology conversation to a major business continuity issue that C-suite leaders must figure out.

CM: *Yes, that makes sense. It's an important issue for all executives but that doesn't mean the CMO has to master all the technical details. Having a working knowledge and a big-picture understanding is what matters, and having the ability to ask insightful, probing questions will be important going forward.*

You've worked with companies that have gone into a panic after a breach and observed their steps. How do they react?

JK: The impact to companies has been variable. For example, at Northrop Grumman, there was no change to the stock price following a breach. Sony, however, was devastated by its high-profile security breach. It took two to three years for Sony's stock to recover. More companies are now asking, in advance, what to do in case a breach occurs.

Legal teams have gotten a lot more involved, but it's still a new conversation in most companies. It requires bold leadership to initiate cybersecurity discussions within companies. Some industries are ready for it and some leaders are ready to initiate discussions, but some fields and industries are not yet ready. We are seeing a change. More law firms are getting involved in identifying responsibilities. We are seeing companies begin to identify what information they need to share externally with customers and with the financial community when a breach occurs. It's important for organizations to

determine how they are going to talk about it with the outside world and the community at large.

CM: *I was enrolled in a health insurance company where a security breach occurred. I first read about it in the newspaper, and only received a terse, one-page letter days or weeks later. Really, it was just an FYI, telling me that my information had been hacked. It was a horrible feeling. I remember thinking, "OK, what now?" It took them a while to send a proper communication offering proactive steps, including LifeLock, and recommending that customers be on the lookout for signs of identity theft. The entire experience was very inadequate.*

JK: I would like to see corporate breaches treated like a vehicle recall. With recalls, customers get a notification, go to the dealer and get the problem fixed. With security breaches, most companies don't even have help desks set up so that a customer can talk with a customer service representative. The level of automation makes it difficult to find help. When your information has been stolen, what do you do? What about when your Social Security number is stolen? In my view, our federal government needs a policy for how to help the citizenry. That hasn't happened yet.

CM: *Plus, the government itself has had breaches. For example, there's the Office of Personnel Management, which was a serious breach.*

JK: Just about everyone who lives in DC was hit by this breach, but there was very little guidance.

CM: *How do you prevent breaches in the first place? I've heard you say that risk management and security management executives don't even work together.*



JK: That's true. Security teams usually focus on cyber failures that happen online because they understand that universe well. In the past, risk officers have focused on financial risk. Risk officers need stronger technical backgrounds and better training so they can become more comfortable guiding organizations. The steps are: 1) assess your risk, and then 2) figure out how to reduce your exposure. This should happen before the organization is breached and it should drive the conversation. CIOs and security teams know how to focus on the more technical aspects of cybersecurity but don't collaborate; they can do a much better job than how they work together today.

CM: *Customer experience and marketing leaders also need to enter the picture. But I imagine it would be a massive effort to get all of them working together if the risk, security, and cyber people aren't even working well together. How do you get collaboration started?*


JK: Enterprises need to realize that security, privacy, and cyber teams need to work as an integrated operation. This is a huge effort for a big company. They need to bring privacy laws into the picture, and figure out a way to give customers access to their own information. But security people want to instead lock everything down. This is at odds with the customer experience leader's desire to build and sustain trust. All of it needs to be brought together within a legal framework, which exists today, but this isn't happening at most organizations. When more organizations

adhere to a legal framework, it will make internal collaboration much better.

CM: *Organizations need to realize how interconnected everything is. It starts with websites, which have added personalization and commerce. Organizations may then go further by tracking their customers' buying behaviors, including where some customers go [through GPS], what their faces look like, what they read on websites, and what ads they look at. While this highly personalized information is being collected, a trusted relationship builds over time between the buyer and seller. But this data is very private, highly confidential, and in the case of Europe, legally restricted. Fears of a possible breach, not to mention an actual breach, can quickly shred that customer trust and intimacy and lead to a major meltdown like the reaction that Sony experienced.*

JK: Correct. There are many laws about privacy and you also need to know where data is traveling. That is a big issue for cloud vendors. One cloud vendor developed a local data store and appointed a firm that functions like a data trustee. The trustee organization will own the data and can prove that it hasn't traveled to a specific country. This business model is going to be adopted fast in the healthcare industry; it must happen. There will be a legal framework that stipulates how it will work. The US government is already talking about electronic security concerns and how to ensure that data is trusted.

[Enterprises] need to bring privacy laws into the picture, and figure out a way to give customers access to their own information.



CM: *What about the glut of technologies that have recently emerged or are right on the cusp of happening: things like smart watches, other wearables, drones for business use, embedded GPS in cars, new virtual technologies, the Internet of Things [IoT] – the list goes on. Is this problematic or will these devices fold into the new security models?*

JK: Historically, security specialists focused on network security but systems have changed significantly with cloud. There's a proliferation of devices – smartphones, the IoT – and all these devices are using the public IT infrastructure to communicate. The sheer volume of activity has driven cybersecurity to the brink; we now must rethink it. Security specialists can't just confine their focus to network security; it's bigger than that. Unfortunately, some of them are using the terms of cybersecurity without knowing what cyber actually means. The question we should be asking is: How do you secure your critical infrastructure?

CM: *I saw the press release on the software defined perimeter and it grabbed my attention. What is the SDP and why is it an improvement over what organizations are currently doing?*

JK: The SDP concept came about by mirroring the security approach used by the Department of Defense [DoD] and the National Security Agency [NSA] in the US government. DoD and intelligence agencies operate on a need-to-know basis, which means if you are cleared and have a need to know, then you can get information. Otherwise, you can't get anything.

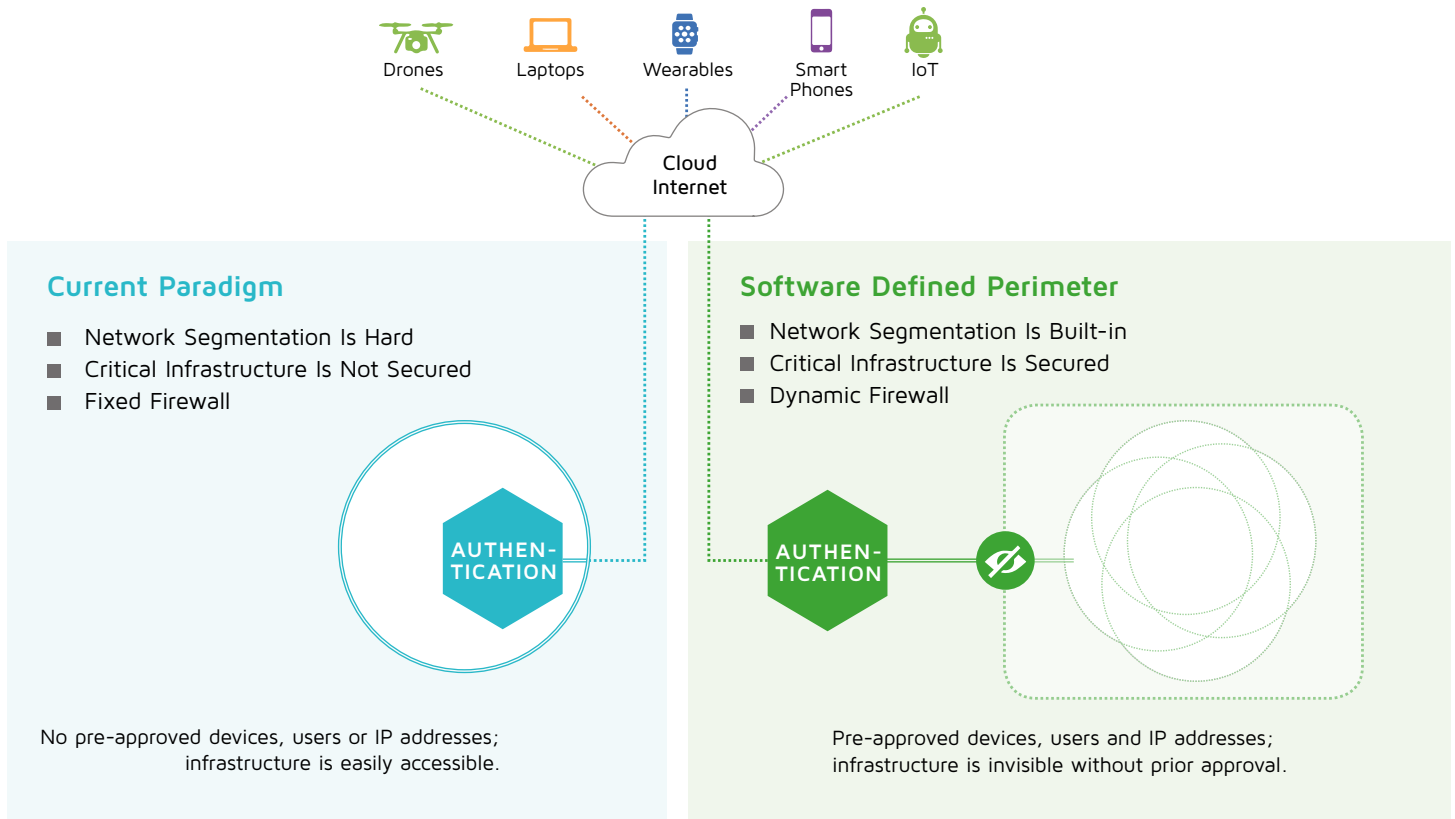
The sheer volume of activity has driven cybersecurity to the brink; we now must rethink it. Security specialists can't just confine their focus to network security; it's bigger than that.

The other DoD concept factored into the software defined perimeter specification is that of fingerprinting devices. [The term “fingerprinting devices” refers to the collection of information about a remote computing device for the purpose of identifying that device.] Combining these two concepts – the need to know and [device] fingerprinting – became the basis for a new architecture known as SDP. SDP maintains an access mechanism to control all the devices tied to users trying to access an organization's infrastructure. SDP is specifically designed to handle the explosion of devices connecting to the internet.

The old paradigm [most organizations use] is to maintain a fixed perimeter with a firewall.⁴ With a fixed system, the organization has control over where or who its users are. That approach is changing now because customers and users want access from phones and laptops, which move around. The perimeter is no longer fixed, because users and devices could be here today and in Russia tomorrow.

The current idea of allowing people to get to your system and then authenticate is really dangerous. With the software defined perimeter, if a user is connecting to a public infrastructure [using the internet or cloud] she must first authenticate her access [user name and device] to even get onto the public network. Secondly, the firm's infrastructure – which in the old paradigm is very public – must be hidden so no one can see it. The software defined

Figure 1
Cybersecurity Architectural Options



perimeter specification defines the idea of a dynamic firewall, which opens and closes to people coming in only if they have prior authentication to even access the firewall. Without prior validation, the user can't get in. And the perimeter completely hides what is behind the firewall so that cyber criminals can't even see the organization's infrastructure - it's completely invisible. The firewall opens up only to people coming in, and then closes. [See Figure 1.]

These are the two key protections provided by the software defined perimeter:


1. Authenticates *users* before they connect to or even see the organization's infrastructure.

2. Authenticates *devices* before they connect to or even see the organization's infrastructure.

Essentially, *what you can't see, you can't hack*.

By eliminating network-based attacks, the organization can focus on its insider threats [like disgruntled employees].

Ideally this is what businesses want to do. Trying to monitor who the hackers are and tracking them down is insurmountable. This isn't a business responsibility; really, tracking down hackers should be the government's responsibility. Today, what we are trying to do is not scalable, is not possible, and the cost is insurmountable.



CM: *Have I got this right: currently, anybody can go to an organization's network, "knock on the door" and the company opens up to decide if they should be authenticated? This is how the bad guys get in? And these companies that are worried about security depend on malware protection to keep track of a constantly changing list of who they should keep out?*

JK: Correct.

CM: *And with the SDP, devices must be authenticated before the system opens up? If I understand this correctly, these two old and new architectures are diametrically opposed ideas.*

JK: Right now, e-mail systems are open, and that works really well. But companies' email systems are riding on the internet, and that is dangerous. Any data that goes on the public network [internet or cloud] is vulnerable. If your organization's mission involves something extremely confidential, such as financial information, military information, and product development, you can't keep putting this information on a public infrastructure because then the onus is on you to protect that information.

CM: *It doesn't take too much imagination to see that a malicious foreign government could hack into power grids, the banking network, emergency services, police departments, transportation systems, and other things that are essential to our way of life and our economy.*

JK: It's happening today. Hackers are very smart, and are constantly working on this. Companies are very busy too, trying to fend off the attacks, but they aren't as smart as the hackers and aren't as focused on it.


CM: *How realistic is it today to use the SDP approach?*

JK: Large companies are embracing it. It's harder for smaller organizations to do. Some level of training will be needed. We hope that infrastructure providers aren't just looking at systems and networks, but also helping companies that are creating the applications that will run on the network. That would make it easier for small companies to embrace SDP. Custom development may need extra work. The way the business and government have architected their networks may make it more difficult to deploy SDP because the application development people are probably separate from the networking people. But over time, hopefully, more adoption will create more services, more products, and more applications that use SDP.

CM: *How much does it cost?*

JK: For a large company, the cost for what would be considered critical for cybersecurity is probably a small percentage of the infrastructure costs. Companies may need to ask, "Where are our biggest risks? Where will we get in the most trouble?" Banks, which need to worry about loans, credit cards, and ATMs, would need cybersecurity for that.

To determine costs, you'd need to estimate by each application and then price that into the architecture. It's possible to get a reference implementation of SDP that is open source, meaning it can be downloaded. Then, the organization would need one to two people to work on the implementation, plus staffing to monitor



and manage it on an ongoing basis. This approach would be a very proactive thing to do.

Organizations already have user accounts and passwords; the team would marry that information to the devices coming in on the network and marry that information to the actual connections. Once again, this is a proactive approach that is based on knowing all the people who are knocking at the door.

It's also possible to break down the IT infrastructure on a smaller basis, and then look at putting perimeters around a subsection, like the supply chain. With this approach you would prioritize the implementations based on criticality.

CM: *Is the cost usually in the one-to-two-million-dollar range?*

JK: Yes, if you are looking at the supply chain. But pricing it is very nascent. A large company may have a million vulnerabilities in its system. It would cost a lot of money to fix all the vulnerabilities. Implementing SDP will be cheaper than fixing all the security vulnerabilities.

CM: *This feels like putting a finger in the dike.*

JK: That's why business leaders must get involved. Organizations need conversations about what their critical assets are, what vulnerabilities are greatest, and then prioritize how to fix them.

CM: *Today, I saw that the National Defense Authorization Act, approved by the Senate in January this year, has a provision tucked into it*

that DoD is no longer required to select the lowest-cost bidder when it comes to cybersecurity. Clearly cybersecurity has moved to high priority within Congress and has impacted spending priorities.

JK: Yes, that is a breakthrough. The understanding [of cybersecurity issues] is moving [expanding among a broader audience].

CM: *Can you say what industries or companies have moved to this new approach?*


JK: Coca-Cola has publicly announced that it has embraced SDP and has moved to the new paradigm. Mazda and Google have adopted SDP by securing their devices that connect to the infrastructure. Groups within the federal government have adopted it too, but have not publicly announced. The Department of Homeland Security is working to solve the denial-of-service problem, and make that available through open source.

CM: *What about telcos and device manufacturers - are they moving faster?*

JK: Yes, conversations are happening regularly with these players because they own much of the infrastructure, even though it is a moving target. As these technologies are moving and morphing, vendors are looking for new ways to protect their bread and butter.

CM: *It's quite scary. Any foreign government with the right skill sets could come after the US, not just the Russians. They could attack the strength of our*

Organizations need conversations about what their critical assets are, what vulnerabilities are greatest, and then prioritize how to fix them.



economy and the very fabric of our government. Hacking public email accounts like Gmail and Yahoo is a scary thought too. Plus, there was that denial of service on the internet last fall that affected consumer devices throughout the country. Are we being overwhelmed by the threat without any way to fight back?

JK: DoD has coined the term “cyberwarfare.” They’ve shown that nuclear power plants are vulnerable. DoD has huge defenses for cyberwarfare, but war really is coming. We have a new Cyber Command [in the military] that is going to take down the covert groups that are attacking us through hacks. DoD doesn’t affect businesses though; they protect the government. But the Department of Homeland Security is mandated to provide cybersecurity through police departments and for businesses. There’s a mind-shift change in the air. But these organizations have to protect themselves first, before they can lead and help others. Putting projects like SDP in place is an example [of protecting the protectors].

CM: *You’ve done a lot with the [Digital Risk Management Institute](#). Could you go over that?*

JK: The reason we started the DRM Institute was to change the conversation for cyber. Instead of trying to think like hackers, why not shift the focus to identifying what kind of risks an organization can bear? This would help companies measure

how much risk they have. Right now, assessing the level of risk is very difficult to do, without changes in how we think. By approaching risk this way, we came up with things organizations can do right away by implementing the right protocols and tools.

But, there is a big concern for CMOs and customer experience leaders. Today, the more secure your organization becomes, the harder it is for customers to do business with you. To move forward, we’ll need to decouple that connection. That’s one thing the DRM Institute is doing; it’s measuring how to keep cyber protection from impacting the customer experience.

This includes developing playbooks. Customer experience leaders would be very interested in the playbooks. We [the DRM Institute] look at things like: How are you going to implement cybersecurity? How do you make sure it happens? Why did you get hacked? Why did emails get hacked? These playbooks are written so that everyone can understand. That’s why we want to talk about risk management instead of focusing so much on hacking.

When you net it out, [understanding the problem and taking proactive precautions] matters a whole lot to the business.

... these organizations have to protect themselves first, before they can lead and help others. Putting projects like SDP in place is an example [of protecting the protectors].

Conclusion: It's Time To Take Proactive Steps

This interview underscores the importance of CMOs and other customer experience leaders taking immediate steps to get involved in cybersecurity planning and measures. The threat to customer information is pervasive, and a breach would put an organization at high risk. Threats range from disgruntled, score-settling employees and identity thieves to sophisticated hackers, corporate espionage spies, and foreign government spies. The risk to customer information and longstanding customer loyalty cannot be overstated.


The most immediate action customer experience leaders can take is to reach out to CROs, CSOs, and CIOs to start a conversation and move to collaboration on this topic. Here are important steps each organization should actualize:

- **Collaborate.** Before any breach occurs, develop an external and internal communications plan and a corporate continuity plan that are ready to deploy as soon as a breach occurs. In the event of a breach, treat it the way companies address product recalls – including setting up a hotline to answer questions and provide help. Immediately work with the security and risk office to jointly issue all correspondence to customers. Prior to a breach, work together to

figure out how to reduce the company's critical cyber risks; e.g., by securing the supply chain, using SDP, etc.

- **Take safeguards.** Prior to any breach, risk of a breach, or thought of a breach, take safeguards that protect customers, starting with never requiring or requesting the customer's Social Security Number (SSN). This is not just a CSO responsibility; CMOs have co-equal responsibility. (However, this is easier said than done because some government agencies require SSNs, even though some states have made it illegal to ask for them. For example, Medicare card numbers are the holders' SSNs, which means that doctors' offices throughout the country have all their patients' SSN data. Honestly, this defies logic.
- **Encrypt customer data.** Safeguard all customer data that is stored digitally by encrypting it and then enforcing limited access to this customer data using strict controls.
- **Be proactive.** Proactively provide guidance to customers about how they can best protect their information, including encrypting their devices. And issue regular information to customers about privacy policies and safeguards.
- **Enforce passwords.** Regularly force password changes, and require an 8-12 digit combination of special characters, numbers, and text. This

The most immediate action customer experience leaders can take is to reach out to CROs, CSOs, and CIOs to start a conversation and move to collaboration on this topic.



is particularly important for remote workers from home, who should change their router passwords daily or weekly if used for work purposes. Apply the same rigor that financial services companies apply, even if you are in a different industry.

- **Safeguard hard copy information.** Make sure your organization doesn't require customers to write down highly sensitive information on paper forms, which can be copied or stolen. Minimize or eliminate the amount of sensitive customer information sent through the mail.

Endnotes

- 1 For more on this topic, see "CMOs, cybersecurity and the criticality of customer trust," <http://www.digitalclaritygroup.com/cmcs-cybersecurity-criticality-customer-trust/>
- 2 For information about the software defined perimeter approach, see the Software Defined Perimeter Working Group, <https://cloudsecurityalliance.org/group/software-defined-perimeter/>
- 3 For more information on the GDPR, see "The Meaning and Impact of the General Data Protection Regulation," <http://www.digitalclaritygroup.com/meaning-impact-general-data-protection-regulation/>
- 4 A firewall is the software and/or hardware component of a computer system and network that is designed to block unauthorized access to or from a private network while permitting authorized outward communication.

About Digital Clarity Group



Digital Clarity Group is a research-based advisory firm focused on the content, technologies, and practices that drive world-class customer experience. Global organizations depend on our insight, reports, and consulting services to help them turn digital disruption into digital advantage. As analysts, we cover the customer experience management (CEM) footprint - those organizational capabilities and competencies that impact the experience delivered to customers and prospects. In our view, the CEM footprint overlays content management, marketing automation, e-commerce, social media management, collaboration, customer relationship management, localization, and search. As consultants, we believe that education and advice leading to successful CEM is only possible by actively engaging with all participants in the CEM solutions ecosystem. In keeping with this philosophy, we work with enterprise adopters of CEM solutions, technology vendors that develop and market CEM systems and tools, and service providers who implement solutions, including systems integrators and digital agencies.

Contact Us

Email:

info@digitalclaritygroup.com

Twitter: [@just_clarity](https://twitter.com/just_clarity)

www.digitalclaritygroup.com