

A Niche with a View into Cyber Incident Response

James Jansen, Consilio



James Jansen

James Jansen leads Cyber Incident Response Services at Consilio, a global leader in eDiscovery and consulting services. As the Global Lead of Cyber Incident Response Services and senior member of Consilio's Client Services team, James focuses on helping clients and their counsel develop and implement effective strategies based on the needs of their matter. Reach him at jjansen@consilio.com

Cyber incident response is a broad market. Where does Consilio sit from a service delivery standpoint?

James Jansen: Consilio has a unique niche that leverages our e-discovery experience for cyber incident response. As a result, we serve as a more reactive service, partnering with incident response firms, breach counsel and insurance carriers who are dealing with cyber incidents.

We provide programmatic data mining, manual review, and notification report generation to our clients and their counsel who are impacted by these incidents. That means that when an incident response firm has conducted its analysis and determined which data has been impacted by a cyber incident, we are brought in and we leverage our data analytics capabilities, our human review resources, and our proprietary technology to generate a notification report for our clients and their breach counsel. That report helps them make decisions about who needs to be notified after an incident. We work very closely with response vendors and the law firms and carriers handling these incidents.

Consilio is known as a leading provider of global e-discovery services. How does your expertise in that area help you assist organizations dealing with by cyber incidents?

At our core, we're an e-discovery provider. That gives us a foundation in terms of technology and data security that is extremely important in this line of service. We're already dealing with clients who are facing a data incident. We can provide a secure environment that's been vetted over the years by some of the largest companies in the world who use us as an e-discovery provider and know their data is secure when they send it to us. We also bring global resources to the table. As a global provider, we have resources not just in North America but in many jurisdictions around the globe, including the UK, Europe and APAC.

Equally important is scale. As more and more organizations are impacted by cyber incidents, service providers need scale to

accommodate the work our clients need us to do. Whether it's technology resources or human resources, scale across the globe is vital.

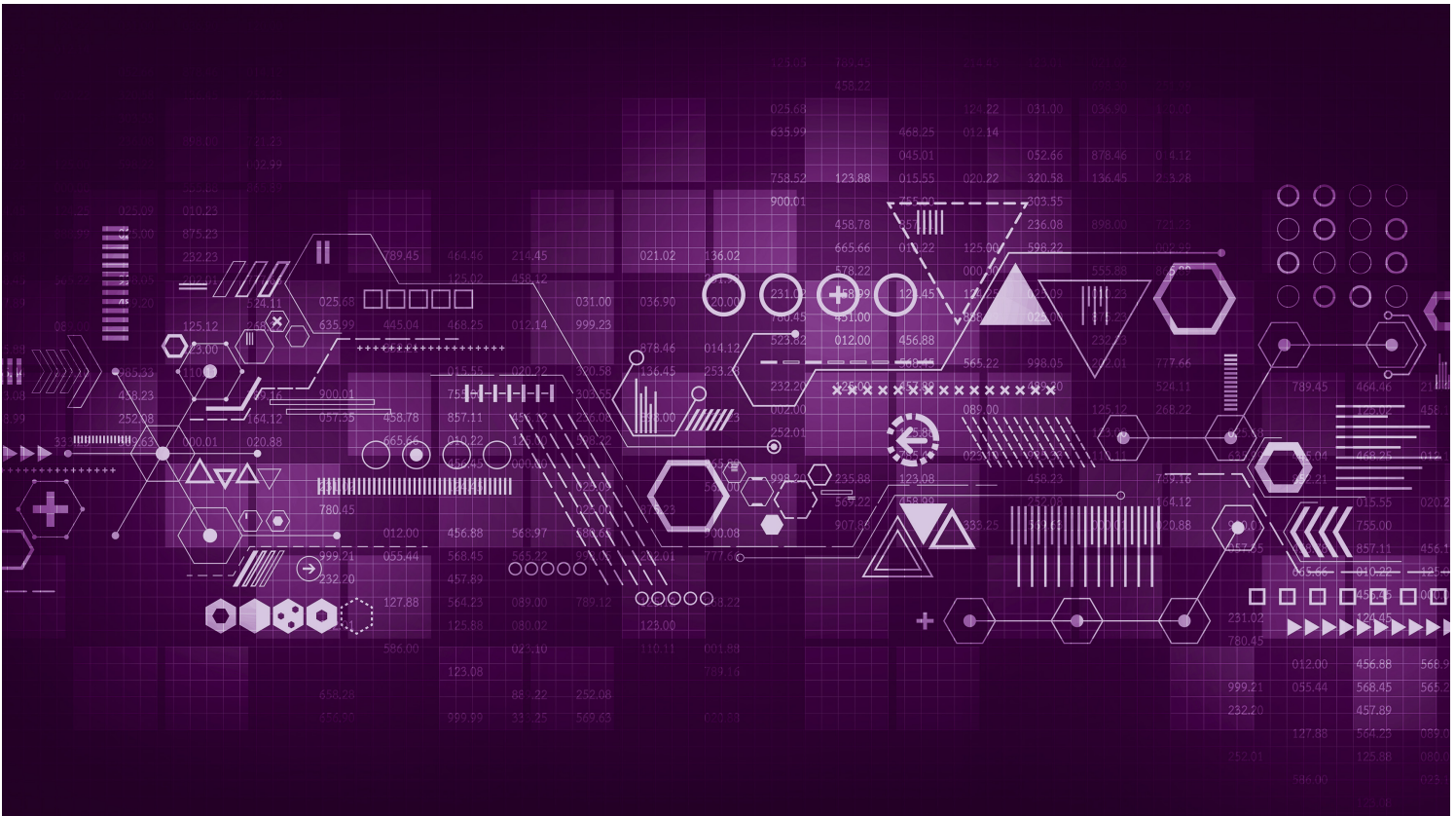
Consilio has recently combined with other organizations. Have these integrations strengthened your offering?

Over the last few years we've merged with a number of organizations. We've been fortunate. Our leadership has brought organizations into our fold that share our culture, our vision, and our commitment to providing impeccable service to clients. When you bring in organizations whose people share your values, including your consultative approach to solving client problems, that's a great fit. We are thoughtful and purposeful about evaluating what

each organization brings to us - whether it's technology that can make our process more efficient, or a workflow process that can drive efficiencies for our clients, it's important to really get under the hood, understand what these additions offer given our current processes, and figure out how they can benefit the organization as a whole. Having gone through a number of these, I can say we are very good at this.

Cyber incidents can be extremely cost sensitive. How does Consilio address this from a technology and resource standpoint?

There are cost sensitivities around these because of the increasing numbers. That's why the work that we're doing



must align with what are our customers – ultimately the carriers and breach counsel – expect as a result.

In addition, when we look at the cost of these matters, it's important to take a holistic view. There's no technology alone that's going to drive efficiency, and there's no human resource component that's going to drive that efficiency all on its own. Therefore, we look at it from a holistic standpoint.

As an e-discovery organization, we realized many years ago that leveraging high-level analytics and having high-level expertise is a key component to help our clients assure they have a defensible and efficient process, and, at the end of the day, that they can get that in a less expensive manner. So we are constantly vetting or looking to build technology that is going to allow us to work more efficiently. For example, we have members of our analytics team with deep experience using more technical scripting than perhaps we generally would use on the e-discovery side of our work. We can identify that kind of skillset within our team, pull it out, and use it to drive efficiencies in cyber incident response. We're always looking for ways, from a technology and resource standpoint, to be more efficient by finding the right people and the right technology to do the work.

As 2022 gets underway, what's the most important thing you can do to help clients facing cyber incidents?

The biggest thing we can do as an organization is to be consultative. When I look at cyber engagements, it's important not to try to fit each incident into the same box. We have a variety of tools and technical capabilities at our disposal. It's important to figure out what's the right fit for each cyber incident we're handling. It may be that a client has unique data sets and we need to leverage multiple resources internally to find the right solution to their particular challenge.

I'll give an example. We had a client that dealt with health insurance claims. The initial discussion was that someone would have to put eyes on all of these records to pull up the relevant information. After discussing this with breach counsel and the client, and bringing in some of our technical resources, we found a custom solution to extract information from 40,000 records without having a single person put eyes on the documents.

Cyber is a rapidly evolving market. What has changed about your service delivery over just the last year or so?

Our clients and their breach counsel are more involved and have higher expectations regarding the initial, upfront data mining and data triage that we're doing on these types of projects. As this evolves, and as the number of incidents increases, it becomes more necessary to drive efficiency. I know I've used that word a great deal, but that's the truth. We need to drive efficiency, shorten timelines, and do things less expensively. One of the key ways to achieve that is being very strategic about addressing these types of projects.

Is there anything that we missed?

I would add that we interact with many different pieces of the "cyber puzzle." There are a number of different seats at the table, and where we sit, we interact with most of them. Our work in the space gives us an interesting perspective, particularly as we deal with the data challenges across all of our many highly varied projects.

As an e-discovery provider, we have a foundation in technology and data security that is extremely important in this line of service.



Let's *evolve* the *agility* of *legal solutions*

Demands are high. Change happens quickly. From decreasing response times to designing legal workflows for scale, Consilio is trusted by over 7,000 global corporations and law firms to swiftly deliver a complete legal consulting & services experience. We invite you to discuss your goals and how we can work together to evolve the future of your legal solutions.

For more, visit consilio.com



*Evolving the future
of legal solutions*