MCC INTERVIEW: Sam Chi / FRONTEO

Are You Bilingual in Cybersecurity?

Lawyers need to learn to speak tech, and IT professionals need to speak legal

***Sam Chi** has been working at the intersection of lawyers and technology for more than 15 years. He spent a decade managing a team of e-discovery technical consultants at Latham & Watkins before moving to **FRONTEO**, where he is a senior vice president in discovery services. He's witnessed the tension that can crop up when IT and Legal are forced to collaborate under the pressure of, say, a data breach. His experience has given him insight into the problems and ideas for solutions. And he thinks in-house lawyers are ideally situated to help make things better. The interview has been edited for length and style.*

MCC: Cybersecurity has been a very big issue in the legal industry for quite a while. In recent years, a lot of attention has been focused on the relationship between in-house lawyers and their outside counsel. Why is that?

Chi: I think it's an economic issue. IT departments within an organization think of things in terms of prevention: preventing hackers, preventing malware, preventing all other cybersecurity threats. The legal department gets involved, typically, in response to a bad situation, whether it be regulatory requirements or lawsuits. So they are more reactive. But I think the more important question is: At what point is there a dialogue between the IT departments and their in-house lawyers and their outside counsel?

At what point is there a dialogue between the IT departments and their in-house lawyers and their outside counsel?

MCC: Early on, law firms seemed slow to respond to the concerns of their clients. Do you think that's a fair assessment?

Chi: I don't think it's a fair characterization to say that law firms are slow in response. Rather, as I said, law firms tend to be reactive. Again, it's more economics – a supply and demand issue. The law firms have, in recent years, addressed cybersecurity and brought it to the forefront as demand has grown from in-house lawyers and corporations.

Just look at what's happened in the last five years: big time cybersecurity issues. For example, the Target matter, where some cyberthieves accessed customer credit card information through a subcontractor. That led to $10 million in damages and a class action lawsuit, $39 million to financial investors and institutions and another $60 some-odd million to a credit card company. I think with the emergence of these lawsuits in recent years, the law firms are now beginning to respond with lawyers who are very knowledgeable in the cybersecurity realm.

MCC: So, you think it took some big headline cases and some very big numbers to get their full attention. Is that what you're saying?

Chi: Yes.

MCC: I guess that could certainly be said of in-house lawyers everywhere. I think if there is someone who isn't paying attention, now, you have to ask what planet they're living on.

Chi: Yes, exactly. And with in-house lawyers – I'm probably going to go a little off-topic here – but FRONTEO is an e-discovery services and consulting provider, so we're on the technical end, serving law firms and corporations. In my former career, I was part of a law firm. One of the biggest disparities I saw was simply communication. IT speaks a different language than Legal. This is not just with cybersecurity, but with information governance, litigation and any other regulatory and legal-type of services. The language disparity and the understanding between the two groups has impeded progress in all avenues where Technology and Legal should be more involved, more transparent and more understanding of each other.

Sam Chi *is senior vice president of discovery services at FRONTEO, where he oversees complex engagements and provides consultation to clients on every phase of electronic discovery. He also has extensive experience consulting with Am Law 100 firms and Fortune 100 clients across a variety of litigation focuses, from regulatory matters to patent litigation, and on multijurisdictional cases spanning the U.S., Europe and Asia. He can be reached at schi@fronteo.com*

MCC: Tell me a little bit about how you think IT departments and law departments have learned to communicate better over the last few years. What has been successful? When have you seen that seems to be working well in some of these instances, and what do you attribute that to?

Chi: Bringing in outside vendors or having internal resources that not only understand the legal issues, but also understand IT can be successful. Law firms have added internal resources to bridge that gap. They've added internal experts who have backgrounds in technology, but also understand the legal issues. They can act as translators, if you will. That was a huge change for law firms and in-house counsel to initiate. Recent lawsuits and requirements have forced IT and legal counsel to start collaborating and talking to each other because the sensitivity of the data and the nature of the data has become so important and crucial that law firms and in-house counsel have been forced to understand these issues.

MCC: So in-house law departments have done the same thing?

Chi: Yes, absolutely. You see this with larger corporations that have evolved, unfortunately, because they've been on the losing side of things. They've either had a security breach or been on the receiving end of a big fine. Some larger corporations with larger in-house legal departments have added technical experts. Smaller companies reach out to outside counsel, and because of these questions and requests to outside counsel, the outside counsel have also added technical experts to their staff.

MCC: Right.

Chi: Now, the smaller law firms will engage outside vendors, but it's a downstream effect where everybody has had to beef up their staffing and expertise in one way or another.

MCC: So, it sounds like if you were advising in-house departments, if they haven't already either hired people in-house who are bilingual in IT and legal, and can translate and function as a liaison, that would be something you would recommend. Or if they're smaller, they find partners who can function that way. That's some of the advice you give companies that are wondering what they can do to more effectively respond to these situations, correct?

Chi: Correct. They should have the resources readily available, whether it's internal, through outside counsel, or through a partnership with a technical services organization. I think at the heart of it, you just simplify everything. As I said earlier, traditionally IT thinks of things from a preventive perspective; it would be beneficial for IT departments to bring in their in-house legal departments or outside counsel and think, "What happens if the preventive maintenance doesn't work? Where are the potential security breaches, what's out exposure and liability?" Thinking not only from a risk perspective, but what types of information can we afford to lose?

MCC: Are in-house lawyers in a good position to encourage and guide that dialogue?

Chi: Absolutely. Being in-house, you're in a position where you have internal knowledge of your organization. Here's the major difference: with in-house legal departments, they need to think of the business model as a whole and the organization as a whole. Whereas with law firms, what they're really thinking about is a matter, whether it's a lawsuit or a legal transaction. The law firms are thinking about that particular project or that particular issue. In-house counsel, on the other hand, are in a position to think about the business in its entirety.

MCC: Yeah, yeah. That puts them in the right frame of mind to figure out how to protect the company as a whole. So, is there other advice you have for, in particular, in-house lawyers who are facing this kind of daunting challenge – this potentially existential risk for a company?

Continued on page 36

After the Breach

Continued from page 00

MCC: Are you seeing more and more encryption and more and more locked devices?

Cancilla: We are. Typically, back in the day, encryption would've been limited to a company computer. Now we're even seeing it on a personal level. People are very aware of their devices and information that they store on those devices, so they password-protect them; they encrypt those devices, which makes it very challenging from the examiner's perspective.

MCC: How have the people you're investigating changed, as far as their level of knowledge and the tools they're using?

Cancilla: They're significantly smarter nowadays with all the information that's available just by going online to Google and looking to see how to counter a forensic investigation. A lot of times, they're able to remotely wipe their devices. If we get our hands on an iPhone, a user could be sitting thousands of miles away and remotely wipe that device if we don't take the proper precautions. They've evolved and gotten smarter so that they know what to do and how to take information so that they've covered their tracks.

MCC: What about your side? What are your most potent tools to counter with these days?

Cancilla: The industry-standard tools that we use would be EnCase, Access Data's forensic tool kit. There are a lot of tools, and the tools are evolving with the technology.

MCC: What do those tools do?

Cancilla: A lot of times they're able to break some of the encryption that we see. They're able to allow us access to the data on the devices so that we can perform our investigations. One program called Cellebrite is able to get into the mobile devices from a file system level, so that we can do an analysis on those devices to see what happened and what may have occurred.

MCC: Who is winning the technology war, the good guys or the bad guys?

Cancilla: That's a tough one. I'd like to think that the good guys are, but the bad guys always seem to be one step ahead in what they do. If someone really wants to get away with something, they're going to find a way to get away with it.

MCC: What are the biggest dangers to companies today?

Cancilla: One of the biggest dangers that we see is the "bring your own device" policy – corporations allow the employees to bring their own mobile devices. Then when employees leave the corporation, those devices go with them – and a lot of times so does intellectual property. That's one of the biggest challenges we see. The other challenge is the integration of cloud storage systems – Dropbox, Google Drive, whatever it may be – where employees have information that can easily, with one click, go right out the door.

MCC: Just from a security standpoint, if you were the CEO of a company that was worried about these potential vulnerabilities, would you ban Dropbox and Google Drive? Would you ban "bring your own devices" from company policy?

Cancilla: A lot of corporations do that. It's a good policy, not to the extent that you don't use those things as a corporation, where you need to have access to them. Bring your own device, by banning that, you're saving a lot of headache when an employee leaves. Dropbox, Google Drive – if there's no reason to be using them in the ordinary course of business, there's no reason that you shouldn't have those banned.

MCC: Have you been in touch with companies that have banned those technologies and heard back about how things were going?

Cancilla: We have. Even here at RVM, we do, to some extent, restrict the use of Dropbox and cloud storage systems. We restrict the use internally of accessing personal email accounts. We also restrict the use of thumb drives being plugged into a computer. We block the common ways for people to copy information and take it with them.

MCC: How have employees responded?

Cancilla: There really hasn't been much pushback on that. As far as the employee's perspective goes, if they don't need the access to that information for the ordinary course of business, there's really no reason to have it.

MCC: What's the best advice you can offer in-house lawyers whose responsibilities include cybersecurity and an overview of this area?

Cancilla: Stay on top of your data retention policies. When we go into corporations, a lot of times we do data collection work for large-scale litigations. Corporations seem to have massive amounts of data that's still available. Stay on top of those retention policies so that when litigation does come down, and we come in to collect, we're not pulling tons and tons of data that may not be relevant, that may be outside of the time period that's relevant. It can save you a ton in costs when that litigation does come down.

Cyberliteracy Gap

Continued from page 33

people on the board who understand what questions to ask. This goes to certification programs, including what NACD is offering, which can help. You don't have to have folks who are deeply technical. It's more of a risk-tolerance discussion.

MCC: Board service has changed over the years. There was a time when you could get away with reading the book and going to the meeting, but no longer. There's a lot of pressure on directors to take a more active, strategic role. What's your take on the demands on directors?

Dunie: It is a difficult job. Understanding market dynamics and developments can require external research that goes beyond the board books, especially for independent directors. But independence also brings the benefit of cross-industry experience that can be relevant. Disruptive market forces like technology and cyber can both enable and deter your strategy. Directors with technology and cyber acumen can be an advantage in the current environment by asking the right questions and exploring context that can provide an opportunity for better board governance.

MCC: Talk about a little more about the bigger picture.

Dunie: Cyber is part of an overarching enterprise risk program. If you're looking purely at cyber, you're missing the big picture. Cyber risk is not just an IT problem. It is an operational problem. Those systems are not necessarily under the CIO, but operational technology is just as vulnerable as the technology overseen by IT.

At the same time, cyber is an incredible enabler. By not engaging in online services, e-commerce and other things to accelerate your business growth, you can leave your company at a competitive disadvantage. It needs to be done thoughtfully, and you need to constantly balance the benefits and the risks of the cyber enterprise, as part of an overarching approach to enterprise risk. And remember that your cyber enterprise also may include your suppliers, subcontractors and consumers.

MCC: To double back to the NACD initiative, given your unique perspective, is it valuable?

Dunie: Cyber is still a relatively new topic for boards. NACD has done a lot to raise the profile and help folks understand that there are things you can be doing. I'm excited about the educational opportunities and certification programs that can assist directors in understanding the landscape and inform good decision-making. NACD is moving the needle in that regard.

Bilingual Cybersecurity

Continued from page 34

Chi: Open dialogue with the respective departments that are in control of digital information is very important. Additionally, often we get so caught up in digital information, we forget about paper. Communicating about paper documentation is also very important.

In-house counsel should start with understanding where the data is in the organization, what it's used for and how it's used, as well as understanding the regulatory requirements by the various government bodies. If it's an international corporation, they have to understand the governing laws and privacy laws for those respective countries. It's hard to get their arms around, but I think the first step is just understanding where things are, where data is stored, whether it's on the cloud, or it's behind their four walls, understanding what data is accessible to subcontractors and their vendors, and understanding which data is critical and which data is less critical. Taking into account the budgetary requirements of the business is critical. Attempting to get their arms around all these issues is key. Also working with outside counsel to understand where their weaknesses are, what their exposure is and to seek any kind of remediation efforts, if they need to, and go from there.

MCC: One more question. One issue floating around is whether a corporation ought to have some designated cybersecurity officer in charge of this whole area. It's a big area with big risks. Do you have an opinion of whether companies ought to designate a chief cybersecurity officer.

Chi: Yes, I do have an opinion. I think that goes back to what I was saying as an internal expert on cybersecurity issues. I think a lot of companies have already started doing that. You're the chief security officer or chief compliance officer who has to be knowledgeable about these areas. A lot of companies have already started doing that. I think it's worthwhile to have that in place.

MCC: Is there a particular kind of background that you'd be looking for from that person?

Chi: From my perspective, someone with an IT background and someone who understands government regulations. It needs to be an expert who understands both sides of the fence – that's critical to bridging the gap between Legal and IT, for sure.

MCC: Well, what about you? Do you see yourself as a candidate for that kind of job?

Chi: I might. I do have the background. I was an IT manager for a number of years, and then went to the legal and e-discovery side of things. It's an area that definitely interests me.