

# Talking With Michael Overly Of Foley & Lardner...

## How to Market a Strategic Legal Service Monopoly

“ ...IT'S NO LONGER ENOUGH TO  
HANG A SHINGLE ON YOUR DOOR  
THAT SAYS, 'INTERNET LAW,' OR  
'INFORMATION TECHNOLOGY.'  
YOU HAVE TO HAVE SOMETHING  
MORE SPECIFIC TO SELL. ”

**M**

idway through our interview with Michael Overly, we were interrupted by an emergency client call. Appropriately enough, the interruption confirmed everything that Mike had been saying about his practice— that it is, in effect, a cyberspatial 9-1-1 requiring immediate response and immediate expertise.

Overly is a partner based in the Los Angeles office of Foley & Lardner, and a member of that global giant's E-Business and Information Technology Group. In 2002, he spearheaded the creation of the Cyber Incident Team, a joint venture with M2000/IS, an information security consultancy.

The Team conducts forensic investigations and provides compliance guidance to companies that, to put it simply, have either gotten hacked or want to ensure that they don't. It's a full-service practice niche with technical assistance to plug security holes and legal counsel to address diverse long-term issues.

The Team's quick success in the last year underscores significant legal profession trends, especially on the technology side. We are, certainly, seeing an ever-increasing demand for ever-greater specialization. Online commerce may still be mired in the aftermath of the dot.com crash but technology progresses apace. Legal services providers must meet the technical challenges if they're to be at all credible in this arena.

It's a trend-line that's put real meat on the marketing bone because it's no longer enough to hang a shingle on your door that says, "Internet Law" or "Information Technology." You have to have something more specific to sell.

Such challenge also presents a salient opportunity to be unique. Overly and his Cyber Incident Team have, in fact, achieved a veritable strategic monopoly. They achieved it by swiftly defining a need, swiftly developing the expertise to address it, and swiftly marketing their solution.

The race is indeed to the swift. By being the first in, the Foley team has outdistanced latecomers to this game. Competitors remain few in number and, for the most part, barely conspicuous on client radar screens, especially in key industries like financial services and health care.

Our conversation with Mike Overly – when it wasn't being interrupted by real-time threats to the global infrastructure– offers lessons in kind for all professional services organizations in search of that holiest of marketing grails called differentiation.

**Edge:** How did the collaboration with M2000/IS evolve?

**Overly:** Like many close collaborations. We had worked together on numerous occasions, respected each other enormously, and, when the time was ripe, we opted for a formal arrangement.

As lawyers, we were advising companies on the legal issues related to computer security. Whenever there is a break-in, it opens a Pandora's box. Does the client have civil redress? Is the client itself actually liable for negligence of some sort? What are the criminal ramifications?

There are disclosure issues. In California, there is a duty to report incidents to all individuals whose privacy or intellectual property may have been compromised. In some instances, companies even have a duty to report to the SEC.

As legal counselors, a lot of our work has also been prophylactic, especially for health care clients, and for the financial services where security is king. We build security provisions into business-to-busi-

ness contracts. We look hard at corporate policies and practices. You'd be surprised, for example, how many companies terminate employees and then don't bother turning off their computer access.

And, as lawyers, we perform a service to clients in these situations that only lawyers can perform: We can sometimes fold the incident into attorney/client privilege and shield the information from being disclosed wherever we are not compelled to disclose. Remember, a cyber incident can really compromise a company's reputation in the marketplace. The less said about it, the better.

For years, clients kept asking us for referrals to security technicians who could jump in at a moment's notice and assess and fix a problem. Meanwhile, M2000's clients kept asking them if they knew any good lawyers. In 2002, we pooled our expertise and proclaimed it to the world.

**E:** I would have thought that, for so critical an issue, clients wouldn't have to look very far for legal counsel.

**O:** Quite to the contrary – and thereby hangs the tale. Think for a minute about the legal marketplace in the last twenty years. How many firms have listed "Internet Law" or "Information Technology" as practice areas? How deep could so many practice areas be?

You mean all those lawyers have advanced technical expertise?

Not likely. More often, an Internet practitioner is, perhaps, just a copyright lawyer applying the same legal principles to an online article as he or she might apply to the hard copy that appears in a magazine.

---

#### ESTABLISH BONA FIDES

---

**E:** What, by contrast, distinguishes your group?

**O:** There are only about a dozen lawyers in the world who have gone through the rigorous process of qualifying as a Certified Information Systems Security Professional (CISSIP). For computer security issues, this benchmark defines real expertise

CISSIP is really a differentiator. It takes three or four years just to earn status to take the test, and then another six months of intensive study. And, after you've gone through this grueling process, it requires 120 hours of continuing education to stay CISSIP-qualified.

Of the dozen or so lawyers who are CISSIP-qualified, two are at Foley.

**E:** Yet when I look at the roster of lawyers at the leading intellectual property boutiques, I see lawyer after lawyer with impressive technical, not just legal, training.

**O:** But not in security. That's how we're different.

**E:** Even with your expertise, the Cyber Incident Team could not be formed strictly from the ranks of Foley & Lardner. You needed M2000 as well.

**O:** Absolutely. And it couldn't just be an outside consultancy that we would rely on, on an as-needed basis. Nor was it enough to staff non-lawyer technical experts on whom the lawyers could rely for support. It had to be a full-blown joint venture.

**E:** Why?

---

“ MORE OFTEN, AN INTERNET PRACTITIONER IS, PERHAPS, JUST A COPYRIGHT LAWYER APPLYING THE SAME LEGAL PRINCIPLES TO AN ONLINE ARTICLE AS HE OR SHE MIGHT APPLY TO THE HARD COPY THAT APPEARS IN A MAGAZINE. ”

**O:** Well, there are a couple of pieces to the puzzle, in terms of how we've been able to more or less monopolize the area. The first piece is that we have unexampled expertise in the area. The second piece is that these cyber incidents are often bet-the-company matters.

On the technical side, we needed unimpeachable resources that go beyond what any law firm is in business to provide. At the same time, because of the urgency of the work, we have to swing these resources into immediate action whenever there's an incident.

There's no time to figure out which technical consultants on our rolodex might be available. There's no time to get to know the people you'll be working with. Midnight Friday, right after an attack, is not the time to start developing a relationship. In order to coordinate a response, the best practice is to be working with someone with whom you have a formal business relationship. Things have got to go like clockwork.

**E:** But patent litigation is often bet-the-company as well.

**O:** Again, patent cases are often handled brilliantly by generalist trial lawyers, supported by technical advisors. Also, a patent case might have a window of months or even years to develop. With cyber security, we're talking about a window of hours.

## DEFINE DEMAND

**E:** So, from a strategic marketing standpoint, it's a potent combination. The work is crucially important, there's very little time to do it, and precious few people who know how to do it.

**O:** Precisely, and by having two qualified provider organizations joined at the hip, we cover those bases.

**E:** How many people are we talking about?

**O:** The Cyber Incident Team includes about a dozen people at Foley & Lardner,

and twenty or so at M2000.

**E:** You mentioned earlier that a company itself may actually be liable for an incident, even though it's the victim.

**O:** Sure. Much of our work is about protecting systems from further intrusion and building systems or mandating policies and practices to keep companies intrusion-proof. But a great deal of our work is also about what we call 'downstream liability.' One company, for instance, was relying on outmoded encryption that made it liable to possible damage claims from anyone using or interfacing with the system.

Or take viruses like "I Love You" and "Melissa." They originated in the Philippines, from a hacker who has no money, probably couldn't be sued anyway, and isn't even subject to criminal prosecution in his own country. But if IBM picks up those viruses, and passes them on to the rest of the world, IBM is the deep pocket that people may go after.

Distributed Denial of Service Attacks are likewise dangerous in terms of protracted liability. When you take down Amazon and eBay, as those services were taken down not so long ago, there are suppliers and business partners all over the world who go down too. They may have strong causes of action if they can demonstrate a lack of proper diligence in protecting against these attacks.

There's statute after statute mandating information security of one sort or another. Graham-Leach-Beily, for example, put such provisions into law before the hacker epidemics began. The regulators are watching the shop as well. The FTC, for one, has stated that unsecured web sites will occasion inquiries and enforcement actions.

**E:** Has terrorism increased interest in your services?

**O:** Since September 11, many companies have indeed been looking more closely at computer security. Just like the hacker in the Philippines, these people are physically unreachable, and, I'm afraid, they don't really need much money.

**E:** I understand the unique advantage that being CISSIP-qualified gives you. Yet, as I listen to you describe the legal and economic exposure that's involved, it is still rather astonishing that you would have a virtual monopoly of work that is so...well, earth-shattering! How planned out was your monopoly?

**O:** Planned out enough so that I understood the crucial importance of the CISSIP-qualification. But there was more at play than a happy coincidence between a profound marketplace need and a certificate that I happened at the time to be interested in getting.

“ OR TAKE VIRUSES LIKE 'I LOVE YOU' AND 'MELISSA.' THEY ORIGINATED IN THE PHILIPPINES, FROM A HACKER WHO HAS NO MONEY, PROBABLY COULDN'T BE SUED ANYWAY, AND ISN'T EVEN SUBJECT TO CRIMINAL PROSECUTION IN HIS OWN COUNTRY. BUT IF IBM PICKS UP THOSE VIRUSES, AND PASSES THEM ON TO THE REST OF THE WORLD, IBM IS THE DEEP POCKET THAT PEOPLE MAY GO AFTER. ”

In a sense, the real strategic marketing begins with talents and capacities that everybody has. As members of Foley's E-Business group, we simply paid a lot of attention to our clients. We clearly saw this need for computer security expertise. We saw that no other major law firms had it.

**E:** Not yet....

---

## SEIZE THE MOMENT

---

**O:** Good point. Once we perceived the need, we took immediate steps to develop the expertise. We pursued the all-important CISSIP-qualification. And, we started writing articles and attending conferences. Maybe others will get into this area, maybe they won't. But it's not something you can buy in the lateral market. We've got a real head start whatever happens.

I'll give you a pointed example. The Secret Service has quarterly seminars on computer and Internet security. As you can imagine, the participants include a rich array of corporate and public interests. Foley & Lardner is the only law firm involved.

**E:** But let's say there are a dozen other American lawyers now on the verge of being CISSIP-qualified. How will you maintain your monopoly then?

**O:** Monopolies don't last forever. But by being first, in an area that requires a lot of time to develop – and by doing the basic marketing things to remind the marketplace who we are – we will, I believe, maintain an advantage.

It's an advantage that you always have when you are able to say to a client or prospect, "Ok, you've spoken to another firm that has handled a critical cyber incident. But what were they doing yesterday? What were they doing last month?"

It's not just that we've done it longer and more often. We do it everyday as well.

---

## EXPLOIT YOUR STRENGTHS

---

**E:** Did you have an advantage to begin with because Foley & Lardner has such a

large financial services and health care client base?

**O:** Sure. That's what strategic planning is all about, at both the firm-wide and practice group level. There was a natural fit. When we began planning what you've been calling our "strategic monopoly," we were encouraged in part by the fact that no one else was doing this work for two of our key industry sectors, financial and health. At the same time, no industry sectors need this work more than financial and health.

Industry-based marketing and practice area marketing should always support each other in that fashion. Again, it was a question of acting fast, as fast as the certification process allowed, so that, a year or two later, we'd be a year or two ahead of everybody else. In this marketplace, a year or two is a long time.

We had an additional advantage as well. Unlike other lawyers, we didn't need to convince anyone that they needed this service. Demand was there. It was an urgent demand.

**E:** Presumably, the buy-in at Foley for the joint venture must have been strong.

**O:** Yes, at many levels. First, there was the clear perception that what we wanted to accomplish was a good fit with who the firm's clients are, and what their needs are. More than a good fit. A vital connection!

As a firm, Foley is predisposed to develop unique, highly niched practice groups. There's a keen sense at our firm of the value of such well-defined niches, and of how these specialized groups need to be integrated, in terms of both the practice itself and our client industries.

As such, we were able to draw expertise from around the firm. What we do involves white collar, privacy rights, HIPAA expertise – a lot of stuff that is not necessarily technical, but directly relevant to a cyber incident.

There's another, very practical reason why we needed strong firm-wide support. Our

practice moves so fast, we can't wait for committees to convene and deliberate and get back to us with a yea or nay six weeks hence. Take conflict checking, for example. If we get a call at midnight on Friday from a new client that needs a remedy by dawn, we've got to turn that wheel at once. We need that conflict check yesterday, and fortunately we can get it that soon at Foley.

**E:** The dozen Foley & Lardner Team members are presumably located in multiple offices.

**O:** Yes, in five or six offices.

**E:** How much bigger do you want to see the Team grow?

**O:** I think it's a perfect size right now. On the one hand, the M2000 collaboration has provided us with the critical depth we need going forward.

In terms of the legal team, ours is a premium practice. Its identity is in its being so special. You can't add on warm bodies for the sake of adding on warm bodies. I think, in general, there's a trend at the better law firms away from sheer leverage, toward value instead.

What we've got, we don't want to dilute. ■



Box 700, 21 Standard Life Centre  
10405 Jasper Avenue  
Edmonton, Canada T5J 3S2  
E-mail: [inquiries@edge.ai](mailto:inquiries@edge.ai)  
Website: [www.edge.ai](http://www.edge.ai)  
North American: 800-944-EDGE  
Other Countries: 402-398-4969