LAWDRAGON

# CYBERSECURITY ROUNDTABLE

*Insights* from Skadden, Arps, Slate, Meagher & Flom LLP / September 2015

## Cyrus Amir-Mokri

My introduction to cybersecurity took place while I was in government, serving at Treasury as assistant secretary for financial institutions. In my time there, cybersecurity became a significant operational risk, and it was important to create a robust information-sharing and technical assistance program, sponsored by the government, to assist the financial institutions. We took a "whole of government" approach to coordinate the work of Treasury with Homeland Security and the law enforcement intelligence community.

My involvement in cybersecurity on the government side continued through the end of my tenure at Treasury in April 2014. Since rejoining Skadden, I've been fortunate to work with people like Stuart, Lisa and Mike to further develop Skadden's cybersecurity practice.

## Lisa Gilford

Since I'm in Los Angeles, my practice has a particular emphasis on class actions in California arising under state consumer laws and statutes. Historically, I represented a number of telecommunications companies and litigated cases arising under the Telephone Consumer Protection Act and the California Invasion of Privacy Act. Over time, that has morphed into the cybersecurity area, as cases now tend to focus on data loss from security breaches.

California continues to be a hot jurisdiction for these types of matters, so I'm increasingly called upon to help clients assess litigation risk arising from the statutes and from cybersecurity threats. I've also had a number of cybersecurity issues arise in the context of large-scale product litigation, where information exchanged securely in the litigation is stolen. I've been working on how to retrieve that information and keep it more secure.

## Stuart Levi

My work in cybersecurity originated through Skadden's privacy practice, which dates back to the first dot-com boom. Companies were starting to wrestle with a number of issues involving the unprecedented amounts of data they were collecting online, including what they were allowed to do with it, what their privacy policies should say and their ability to move data around the world. U.S. companies also were struggling with how to run a global business when certain countries and regions, particularly the EU, had far more stringent privacy regimes.

Over the last few years we have added a robust cybersecurity practice. It started with clients who experienced inadvertent data loss, such as data that was accidentally sent by their vendor to another customer. Then they began to experience actual cyberattacks, such as data breaches and denial-of-service attacks. Today, there's a steady drumbeat of these issues.

## Michael Scudder

I first began to work in cybersecurity on the policy side, when I served as the general counsel of the National Security Council in the George W. Bush administration. There were the beginnings of a heightened focus and policy initiatives in the cyber area at that time.

When I joined Skadden in 2009, I wanted cybersecurity to be part of my practice, though not to the exclusion of other areas. I focus on the law enforcement and government-interfacing side of cyber matters. I was a federal prosecutor in the Southern District of New York before working in Washington and have a lot of experience interfacing with the law enforcement community. I still have all of my security clearances from working for President Bush, and I've had a number of matters where I've worked in the classified space for clients.

PHOTOS: DAVE CROSS PHOTOGRAPHY, LIFE IZ PHOTOGRAPHY, KATIE BASIL PHOTOGRAPHY

Lawdragon recently had the opportunity to talk to some of the top minds in cybersecurity at Skadden. The four lawyers reflect the range of practitioners addressing one of today's most pressing topics: threats to vast computer networks and repositories of digital information with the potential to significantly impact enterprises of all sizes and across all industries.

**LAWDRAGON: Let's start by looking at some of the trends you see in cybersecurity today.**

**AMIR-MOKRI:** In terms of where the threat is coming from, the trend over the last year or two has been that cyberattacks are perpetrated by either state actors or their proxies, or criminal gangs that may or may not be related to proxies of state actors. In many ways, we deal with a very murky world, but the reality is that attempted intrusions occur all the time.

I was speaking to a chief risk officer at a major financial institution about a year and a half ago. He said they were facing about 5,000 to 6,000 attempted intrusions each day. That may not be 5,000 or 6,000 different people, but it's still a staggering amount of attempts to get in.

What intruders want to do once they do get in is a different issue: anything from simple spying to exfiltration of data to compromise of data. What people worry about most is destruction, irretrievable destruction — we haven't seen a heck of a lot of that yet, but it's something to watch for.

**LEVI:** Another trend, from a U.S. regulatory perspective, is that the Federal Trade Commission, using its authority under Section 5, has been increasingly aggressive in pursuing companies for cybersecurity violations. In some cases, they are going after businesses that have arguably misled consumers by overstating the cybersecurity protection they offer. Companies find this frustrating because there is no set standard. It's not like the FTC can pull out a document and say, "You are required to take seven steps. You took four. Clearly you misled consumers who would have thought you took all seven." In the view of many companies, the FTC is making it up as they go along. It also can be troubling when the FTC goes after a company that has experienced a cybersecurity incident and asserts that the company has engaged in unfair practices. Again, without a set standard, it's difficult for companies to know what level of protection they must offer.

**SCUDDER:** There is a clear trend of companies properly viewing cyber risk as an enterprise risk — one requiring the attention of not just IT departments but also executive suites and boardrooms. While the right risk management recipe differs from company to company, companies continue to crave the identification of best practices. The challenge, of course, is that best practices in the cybersecurity area evolve as fast as they are identified, making the management of cyber risk all the more difficult. One key to staying ahead is developing the most complete understanding possible of the threats facing an organization. On this front, we'll continue to see many companies more proactively foster relationships with law enforcement and, in many instances, the intelligence community all in an effort to enhance the government's sharing of relevant cyber threat information affecting industry. The trend of enhanced and more robust public-private partnerships, in other words, is one I see continuing with increased energy.

**LD: There's a murkiness that is now affecting every company and government, and individuals as well, and regulatory agencies are racing to keep up. There are no evolved standards. Lawyering on cybersecurity issues must be fascinating because you're working with and creating law constantly.**


Gilford

PHOTO: JOCK MCDONALD PHOTOGRAPHY

**LEVI:** That's right. Every company is vulnerable to attack, regardless of whether they are a financial service institution or a manufacturing business or a professional services firm. All too often, companies think that if they don't have consumers' personal information, their risk is low. They forget about theft of confidential business information, denial-of-service attacks and other cyber incidents that might impact them. These attacks are not limited to large companies. Clients of every size and in every industry are getting hit.

**GILFORD:** One of the major trends I see, and this is probably not a surprise given my background as a product liability lawyer, is the convergence of cybersecurity and product liability law. There are so many devices and products that are now connected to the Internet that are not computers or storage devices, and they're involved in cybersecurity cases and regulation because of their susceptibility to hacking.

There was a recent case against a number of hotels because someone demonstrated how easy it is to engineer access through key cards to rooms. The automobile industry has been hit with a class action regarding the vulnerability of electronic control systems on cars to hacking. We will see plaintiffs' lawyers try increasingly to make hackability the equivalent to liability. It will hit industries we hadn't previously viewed as being subject to cybersecurity threats and issues.

**AMIR-MOKRI:** Another trend is various regulatory agencies coming out either with sets of cybersecurity expectations or guidelines. That's beyond what's going on in terms of attacks and attack vectors and actors. The independent federal agencies and self-regulatory organizations like FINRA (the Financial Industry Regulatory Authority) and others have been issuing guidelines of expected conduct, though none are necessarily raised to the level of hard-and-fast regulatory requirements by which conduct would be assessed.

There's one partial exception — the SEC's Regulation SCI (Systems Compliance and Integrity), which is really a systems-integrity regulation that goes beyond cybersecurity. With the 2014 release of the Department of Commerce's "Framework for Improving Critical Infrastructure Cybersecurity" and follow-up by various regulatory agencies, people are beginning to get a sense of what the expectations are around governance, cyber hygiene, participation in information-sharing mechanisms and crisis management when an event occurs. That includes communication with government agencies.

The financial sector is probably further along than many other sectors in this respect. I think the Department of Commerce's publication is a trendsetter. What remains to be seen is whether adherence to these practices will serve as defenses to claims of liability. Certainly, in a world where conduct is measured by due care or other such standards, these evolving guidelines and pronouncements by regulatory agencies are going to play a role.

**LD: It also looks as though the product liability and class action bars have unlimited potential to create a new cause of action against companies — whether it's security class actions or product liability — with data as the resource, and lack of disclosure of the risks in their management of that resource. Perhaps you could offer some insight on the scale of what you see regarding the growth of claims in that area.**

**GILFORD:** The FTC recently came out with guidelines on the responsibilities of companies that have products connected to the Internet and may be susceptible to breaches. That created a playbook for plaintiffs' lawyers, and I've seen the plaintiffs'

"The FTC recently came out with guidelines on the responsibilities of companies that have products connected to the Internet and may be susceptible to breaches. That created a playbook for plaintiffs' lawyers."

– Lisa Gilford

bar mobilizing around potential targets based on exactly the risks you indicated.

There's a recognition that devices, including pacemakers and other medical devices that are implanted in human beings, wearable computers, watches, cars and hotel rooms, carry the potential for liability. When the FTC issues its guidance, it really does create a "who to sue next" for the plaintiffs' bar.

**LEVI:** The interesting counterbalance is that, for the most part, the plaintiffs' bar has not been particularly successful in these cases. A big reason is that they've had tremendous difficulty establishing "standing" to bring lawsuits, since consumers are generally not injured by these attacks.

For example, in the Target breach, which many consider to be among the worst data breaches in the last few years, very few consumers were impacted financially. Despite all the fear and concern, consumers didn't suffer identity theft, and while many experienced fraudulent charges, these typically got wiped off their accounts.

Now, when they want to bring a class action suit against Target, they are presented with the very real and difficult challenge of showing the court how they were injured. Plaintiffs have tried a variety of approaches to overcome this hurdle, but with only limited success. For example, they might assert that they are concerned about the possibility of future identity theft. This "what if" argument is difficult to sustain, although the Seventh Circuit was recently persuaded by it. In other cases, consumers might argue that they were injured because they spent money on identity theft protection, but many companies now offer that service for free after a data breach.

The net result is that, even in data breaches impacting millions of people, class action lawyers are finding limited financial damage. This means that these cases are settling for relatively low amounts, which might make them unattractive to plaintiffs' lawyers as time goes on. It's not as lucrative as I think they were hoping when this wave of data breaches first hit. It will be interesting to see if interest in data breach class actions wanes over time.

**GILFORD:** As the regulatory environment changes and the statutory basis for certain claims changes, the courts are adopting a broader view of what constitutes standing or the right to sue and what may constitute damage.

As this evolves, you may see plaintiffs' lawyers getting some traction based on the regulatory environment and the theory that products aren't as safe as promised and are worth less than what the consumer believed them to be when they purchased them. This may morph and the idea of a security threat constituting some basis for liability may develop over time. While the plaintiffs' lawyers haven't been doing well in these cases so far, I'm not sure that's going to remain the case much longer.

Given this environment, our clients — no matter what industry they're in — would be wise to think about the way they're disclosing information about products and, frankly, the way they're designing them.

**AMIR-MOKRI:** The concept of loss and damage is important. When you think about some of the debit card/credit card theft situations, the fact is that the financial services industry has become very good at doing two things in this regard: Once a compromise has occurred, they shut down the affected accounts; and the second is fraud detection. Even before the consumer knows there's a breach, they detect unusual activity very well and they shut down the ability to transact.

Part of the loss minimization in these fact patterns is the result of the relevant entities and institutions already working on damage mitigation.

Lisa's point is very important — not just in the financial services industry, but also in other industries: People should think about what could possibly go wrong if there were a breach and ways to mitigate potential damage if something bad happens. Hopefully, the fact patterns will not be worse than what we've seen happen thus far in the financial services industry; even though there has been some loss, it has not been catastrophic.

**LEVI:** In addition to counseling companies in the midst of a data security incident, a significant piece of our practice is advising companies how to best prepare to deal with an attack on the enterprise-wide level. We also advise clients on how to find "smoking guns," such as badly worded statements or policies that were not followed that could be used against them in the event of litigation.

The biggest change in the environment is that clients are much more attuned to the need to be prepared. A year or 18 months ago, most of our clients would say, "Preparedness is interesting; it's probably something we should be thinking about at some point." Now, they are much more actively engaging and, in almost an urgent sort of way, wanting to do something about this.

**LD: To what do you attribute this urgency for preparedness? Have some of the high-profile attacks raised client awareness? Or is it that the firm and others have effectively raised awareness that this is really something clients need to get front and center on? Is it government regulation? A variety of factors could have caused this to come to the fore.**

**AMIR-MOKRI:** It's a combination of all of the above. The spectacular-type events tend to grab everyone's attention. Then the fallout is not just litigation in state or federal court but also congressional investigations, regulatory investigations, reputational risk.


Levi

PHOTO: DAVE CROSS PHOTOGRAPHY

> "We urge clients to have a cybersecurity incident response plan. We tell them it's gone from a 'nice to have' to a baseline requirement."
>
> – Stuart Levi

Every journalist is going to be interested in what happened and how it happened. Senior managers who are concerned about the share performance of their company, if it's a public company, or just the company's reputation generally, are going to be focused on this if they aren't already.

Over the past couple of years, senior management and boards have become particularly conscious of the cyber threat. President Obama's executive order on this subject was issued in February 2013. Headline-grabbing incidents and regulators have made this more top of mind in the last couple of years. Directors and other participants have identified it as one of their top priorities.

Boards are wondering, "What exactly do we need to do? We have our governance structure put together. Now what should we worry about?" People are becoming a little more systematic in their thinking and a little more intent on getting it wherever they need it to be in order to be prepared.

**SCUDDER:** A lot of companies have realized they're not exempt from the risk, that it's not a risk that is only going to present itself in acute ways in particular industries. It's not limited to retail, financial services or energy. We're seeing a lot of companies that operate in industries where their intuition may tell them, "Sure, it's a risk, but it's one that's manageable and not all that acute." Then they're surprised when they have an incident.

For example, a manufacturing company in the Midwest had a particular intrusion about accessing corporate funds, a big company that in complete good faith viewed cybersecurity as a secondary-level risk. A lot of those kinds of institutions are realizing that it's an enterprise risk.

**LEVI:** You'll see every so often — and Sony is the best example of this — an incident that shakes up an entire industry. That hack had a profound impact. It wasn't that North Korea was the alleged perpetrator; it was that the attack happened within the entertainment world. These companies are traditionally focused on piracy of their creative works, but outside of their IT groups for the most part had not focused on broader issues of cybersecurity.

Now we see tremendous focus on cybersecurity by the entertainment industry. They realize how much personal information is floating around — very sensitive personal information that could have a profound reputational impact on a company if it were released. Every so often you'll have an incident like the one involving Sony, which makes an industry suddenly hyperfocused on this issue.

**LD: Is there a basic playbook for what you tell a company, a general counsel or a CEO they need to have in place from a defense perspective?**

**LEVI:** We urge clients to have a cybersecurity incident response plan. We tell them it's gone from a "nice to have" to a baseline requirement. Indeed, today, if you don't have a plan, you are quickly becoming an outlier.

We provide clients with a template to help them think through the key issues. We also get involved in tabletop exercises and walk clients through different scenarios. This ranges from figuring out who should be sitting at the table and making decisions if a major attack occurs to what your legal obligations and responsibilities are.

I'll give you an example of something that gives clients pause. We recommend that they diligence their third-party agreements to see if they're obliged to disclose a cyberattack to business partners, vendors and customers. Inevitably the client says, "Oh, we don't have time to do that now." We tell them, "You can either do it now or in the midst of an attack when there are a lot of other things you're worried about." They realize they really do need to think about these issues and plan.

Clients that have an incident response plan and have tabletop tested it are much more adept at responding to an incident than those that spend the first 48 hours arguing internally over whose area this falls into, who's making the decisions, who should be at the table and which stakeholders are involved. All those questions represent time that's lost in an environment in which you need to move quickly, and it increases the chance of a misstep.

**SCUDDER:** There is no set playbook, but there are certain practices and resources companies need to have in place from a defense perspective. When we're asked to evaluate incident response plans, we invariably find that the plans are too narrow because they fail to address scenarios that may in fact befall a company. Incident response needs to be viewed broadly —

companies need to consider not only operating continuity and information and system safeguarding, but also communications with consumers and other constituents as well as regulators and law enforcement. It's often prudent to map out how communications will flow up the chain within a company during or in immediate response to an incident. This will help organizations avoid certain pitfalls, such as when a company puts together an incident response plan that is very U.S. resource-centric, and a serious intrusion occurs in Europe — basic things like different time zones can slow down a response and the mobilization of resources.

**LD: Lisa, from a litigator's perspective, is it fair to say you prefer to defend companies with an incident response plan?**

**GILFORD:** That's certainly fair to say. Companies find that when they have an adequate response in place, it goes a long way toward defeating claims and eliminating or minimizing damages. Companies are in much better stead defending against class actions if they have quick notification response plans when cyberattacks occur.

**LD: Do you also recommend cyber insurance now?**

**LEVI:** We have insurance lawyers at Skadden who've been advising clients fairly regularly on cyber insurance plans so they understand what's covered and what's not. Also, as companies have incidents, we review their policies and advise on whether they have a claim and how they should approach their insurance provider. That's clearly a large and growing area.

**LD: Is it your estimation that basically all companies need some level of cyber insurance?**

**AMIR-MOKRI:** As good as your defenses are, the reality is that someone at some point is going to penetrate. The questions are, "What is the harm that is done and what is the damage that's done?"

The issue with cyber insurance is that some insurance companies find it very difficult to price it because of the lack of experience. I imagine as the insurance industry builds a bank of experience, this will become easier. We have to wait and see.

**LD: It sounds as though your advice broadly to clients is that they look at an incident not as a matter of if, but when. Two of the areas that we could untangle a bit are how you advise clients to prepare to address the incident publicly, and with the media, since it's going to come out one way or the other, and what the obligations are in terms of public reporting, government notification and how you advise your clients to handle them.**

**AMIR-MOKRI:** It's important to think about what the incident response plan really does and how it fits into the damages scenario. The idea behind it is, once there is an incident, knowing how to mobilize everyone to do everything that needs to get done. Where it becomes very important is in mitigation.

If you have a plan, you can take action to cut off certain activities or operations to minimize the amount of damage that's already going to be occurring. Those first 24, 48, 72 hours can make a huge difference because things happen so rapidly in information technology. If you find out immediately what's going on and you're able to shut it down, it could make a very, very substantial difference between something manageable and something that gets out of control.

A certain amount of damage will already be done. That's the definition of an incident, but the importance of incident response plans is that they can sometimes mean the difference between catastrophic and not.

**LEVI:** A lot of our clients will get a PR agency involved with the media piece. After an attack, we look very carefully at clients' communications. We urge them not to say things very definitively because they run the risk of painting themselves into a corner. These situations are much more in flux than even they realize. Statements need to be phrased very carefully.

**GILFORD:** It's very important that a client's incident response plan take into account jurisdiction-specific rules that guide data breach notification requirements. The California Legislature, for example, has been very active in this area, and data breach notification rules in the state seem to be amended on a yearly basis. It's critical that incident response plans be kept up to date. In terms of broader notification of an incident to the public through the media, as Stuart mentioned, litigation is frequently on the horizon for a company that has experienced a breach, and careful vetting of media statements is crucial.

**SCUDDER:** Companies often have a very real and urgent need to communicate with their customer base. They're inclined to plant their feet on facts before all the facts are out and they're aware of the full scope of the intrusion, and before they've decided as an institution what measures they're going to take to mitigate losses that may appear to exist in the initial phases. So often, clients say, "We have to go in this particular direction" before they've got their arms around the situation. We've even seen it before the incident is complete.

As far as the government goes, most companies in regulated industries will want to think through whether to self-report the incident to the regulatory authority that has jurisdiction over them. They'll also want to consider reporting the incident to law enforcement.

We don't advise clients to reflexively report or not report an incident. Sometimes that surprises people. There are a lot of occasions in which you would choose to report an incident to law enforcement in the very earliest phases. There are other times when you may not. You've got to run through a calculus about what is in the company's best interest at a particular point in time. You can always defer reporting. You can always choose to not report it and allow the government to come to you, and hope things work out fine. So much depends on your capacity to deal with law enforcement at a particular moment in time and what information you feel comfortable providing on a voluntary basis.

Often clients will say, "Why wouldn't you just instantly pick up the phone and let the government know? How does that harm you?" It may set you back some operationally.

**AMIR-MOKRI:** It's a complicated question. You have many different stakeholders. Before reaching out, you have to think about the nature and quality of the information you have and assess what that information

really means, how certain it is, how helpful it is and what its implications are.

There are certain statutes to follow. For example, security-breach statutes create an obligation to self-report if customer information gets compromised. Hopefully Congress will act, and we'll have a uniform standard across the board. At least that will bring certainty as to how people should act in these situations.

Relationships with customers are one thing. Relationships with government agencies are another. Law enforcement presents certain questions. Regulatory agencies present others. At the government, we were very worried about the integrity of the financial system, that a compromise or data destruction at one financial institution could have contagion effects across all of them because they're interconnected operationally. We wanted to know immediately if there was anything wrong from a safety-and-soundness perspective.

We didn't want to get information about every conceivable incident because that's just noise. As Mike said, you have to take a look at the quality of the information and make a judgment as to whether it needs to be shared. Hypothetically, if you find a certain kind of malware or zero-day exploit on your system, you definitely want to let others know this capability is out there that can be used to compromise their systems. That's something people would want to know to protect themselves in general.

The FBI has stated on a number of occasions that they view companies that have been breached as victims. The old view is that law enforcement is going to come, look for something bad and build a case against you. But it's important to step back and think about how law enforcement may be able to help. When I was at Treasury, that's certainly how we viewed it. Often, law enforcement is able to give technical assistance that others can't to help you through a crisis. Self-reporting is an important decision that requires thinking in a textured way about the different stakeholders and the circumstances under which you would reach out to them.

**SCUDDER:** That's a really important point because a lot of institutions will be very reluctant to invite the FBI in, precisely because of their concern that the FBI is going to want to figuratively turn the place upside down — be disruptive and assign blame.

We had a client in the Midwest that had an intrusion resulting in the wire transfer of money out of the company. It was all wired to the individuals that perpetrated the hack itself. After talking to us, the company decided to get the FBI in there right away. The FBI actually knew exactly how the intrusion happened, where the vulnerability was in the company's system. There are instances where the government can add value. That's an essential part of the public-private partnership that you've heard the government talk so much about in the cyber area.

**LD: Mike, when you're talking about the "Do we or do we not self-report?" situation, what would be the reasons on the "don't report" side of the table? Or to you, is it just a clear, "You need to get law enforcement in on this?"**

**SCUDDER:** In the case of the intrusion at the Midwest company resulting in the wire transfer, the situation was one where we thought, on balance, that it should be reported. In other cases, it becomes a question of when. You have to look at how the incident occurred. There's obviously a problem if somebody is able to infiltrate the system and send a fictitious email that results in a wire transfer going out of the company. You could say, "We need to figure out as an institution how it happened and put a plug in it because the moment we invite in law enforcement, they'll only look at it from the standpoint of investigating a crime. We don't have the bandwidth and capacity to simultaneously attend responsibly to law enforcement and deal with the technical decisions that obviously need to be made."

> "We don't advise clients to reflexively report or not report an incident. There are a lot of occasions in which you would choose to report an incident to law enforcement in the very earliest phases. There are other times when you may not."
>
> — Michael Scudder

The company in this particular situation thought they might benefit from the perspective of law enforcement because it looked like something this company would not have been the only one to experience. They turned out to be right.

**LD: It strikes me that among the factors on the side of reporting is if you're in a more regulated environment, like financial institutions, or if it is the kind of intrusion that has the potential to be more systemic or is the first in a series. For instance, with this company, Mike, where they arranged one transfer, if you hadn't gotten on it early, there could have been more transfers.**

**SCUDDER:** Exactly. Stuart and I were involved in a situation where there was a little more hesitancy in informing the government right away because the intrusion was so disruptive to company operations. In the early chapters of the incident, the company was much more focused on what was actually happening at the time and getting their arms around it.

**LEVI:** The incident Mike's talking about also goes to the concern that the FBI would have the mindset, "While we're here, let's see


PHOTO: KATIE BASIL PHOTOGRAPHY

if there are any crimes you might have committed." Also there was a fear that the FBI would walk in and say, "Everybody get up from your desks. We're going to put agents at all the computers and start looking at everything you're doing." We tried to convince them that it wasn't going to work that way.

The other hesitancy — which was interesting, and I think they'll admit they were very wrong about this — came from it being a technology-intensive company. Their view was, "What could the FBI possibly tell us that our very smart technologists and internal cybersecurity people can't figure out on their own?" After we convinced the client to inform the government, the FBI said, "We've seen this exact attack before. Here's what they're after. Here's what's going to happen next. Here's their profile," which of course the company's guys couldn't know. It's not what they do for a living. They were surprised at the utility of the information and the recommendations that they got. We talk about this particular incident a lot because it demonstrates the importance of sharing information and the breadth of knowledge the FBI and law enforcement can bring.

**LD: It's striking how narrow a company's perspective can become when under attack — all the company can see is that it's being attacked. One of the benefits of bringing in outside lawyers and, in appropriate circumstances, law enforcement, is to gain a more objective view — a longer lens than any individual company has on its own.**

AMIR-MOKRI: That's a very important point. That's the perspective of government: to look at the system and at everyone, then say, "Eight other companies were affected by the same thing." When you're in a company, as much as you strive to be aware of what's going on with others, you just don't have the same vantage point.

**LD: That perspective is also critical, I would think, to the board of directors. You advise the CEO and the in-house lawyer and technology leaders, but you may also advise the board. What's most important about your guidance in that area?**

AMIR-MOKRI: A lot of recent cases involve allegations of breach of fiduciary duty. Senior managers and boards of directors have to worry about the fiduciary duty of care, which is, "Are you conducting the affairs of the corporation in a reasonable way?" Boards are trying to think through a lot of issues in terms of how to set up a governance structure.

We also discuss whether a client's primary focus is rapid response or preparedness. How do you conduct the day-to-day affairs of the corporation in a way that's sensitive to information security needs? When should issues be escalated? What's the chain of command? Who's responsible? It's important to tighten up all of the corporation's governance and practices around those kinds of fundamental issues. Taking stock of information security is going to be an essential feature of the company's operations.

When I was at Treasury, we worked with some of the trade associations on these questions. On one occasion, SIFMA (the Securities Industry and Financial Markets Association) took the lead in a simulation of what would happen to the market if there was a cyberattack on it and how market participants would react.

**LD: What were some of your takeaways from that simulation?**

AMIR-MOKRI: It was very interesting to listen to the interaction between the IT people and the business people. The IT people are familiar with the operational aspect and

the guts of what's going on, but the business people have to make the ultimate decision. Does the company continue functioning? If so, how does it function? What message has to be delivered? What are the big business decisions that have to be made?

Every company needs to be aware of these questions because the answers determine the design of their governance structure with regard to information security. Once a company has its governance structure set up, it needs to ask questions such as, "What specifically as a board member do I need to know about how we're doing in terms of information security? What kinds of experts should we be consulting?" These are all evolving issues people are trying to understand better.

Information security is very technical and can get so complex. It's imperative to be able to translate technical language into a medium that is readily understood by business decision-makers, to give them the knowledge they need to make good decisions.

**LD: When you focus on what you report, does the board need to be notified of everything?**

**LEVI:** That's a great question and one clients ask us a lot. Not everything needs to be reported.

You don't need to report run-of-the-mill incidents, such as a small attack that was thwarted. You should report the major reputational-impact-type attacks that could have a material impact on the company. You don't want to call the board every time, but you should call them when an incident rises to a certain level of importance.

It's a challenge. Even if you don't tell the board immediately, you might discuss it at the next meeting. You might say, "Over the last quarter, we dealt with the following couple of issues. Here are the steps we're taking to try to stop that from happening in the future."

**LD: Lisa, do you have a read on what the board should be told from the perspective of defending corporations in class actions? Is there a certain level of reporting to the board that is helpful or unhelpful?**

**GILFORD:** I get involved when there are litigation updates that might be significant to report to boards. In terms of the initial breach and what risks may flow from it, including the risk of litigation, what Stuart and Cyrus have outlined is absolutely where the company needs to be. As they mentioned, it's not a one-size-fits-all construct. It really does involve assessing the situation and getting a good sense of what rises to the level of board reporting and when to report it.

**LD: If a company does self-report, is there a sense that that will result in enforcement agencies looking at it more favorably?**

**AMIR-MOKRI:** As a general matter, many enforcement agencies say, "If you self-report, we will look more favorably because it shows that your compliance and other systems are working." I don't think anyone has made a particular pronouncement in the cyber area, but as a general rule self-reporting is better received than not.

In terms of self-reporting, there's also a more general point to be made. I'm thinking about financial services, which is obviously my orientation. When you have a safety-and-soundness relationship with your regulator, there are two ways to view the relationship. One is adversarial, broadly speaking. The other is a partnership of sorts, where you're trying to use the regulator to help you think through the situation and have an open line of communication to ensure the best results for the company and the system.

Each fact pattern is going to merit its own analysis. On balance, I consider sharing with your regulator a good idea. Again, you have to think about the specific situation, what the implications are, how significant the incident is and when the time is right. All those questions are very important.

**LD: Shall we turn to the future? What is your sense in the near term about how much cybersecurity threats and this practice area are going to grow and in what ways — the predictable and some that folks might not foresee? And then, a bit further down the road, do you think cybersecurity is going to be an area that dominates litigation? Or is it something that will be managed and just one more area of corporate risk?**

**LEVI:** It's hard to say. A lot will depend on the regulatory/legislative point of view, what is enacted or not enacted. That could create a whole slew of new issues.

We're advising a number of companies that have done virtually no work in this area or have done some but only skimmed the surface. As cybersecurity issues and our clients' businesses evolve, we'll need to work with them to update their systems of policies, procedures and governance.

Some clients are more on top of cybersecurity issues than others, but then they say, "We did something in 2012 and haven't really gone back to look at it." They realize as they look at it now that none of it makes sense because they reorganized their business or their risk profile has changed.

**AMIR-MOKRI:** There are two, probably three, vectors to consider when thinking about what might happen in the future. One is, "What are the legal standards and what are the liability rules?" Stuart is exactly right. We have to wait and see how these develop, in court cases and statutes. Congress has been trying to pass a cyber bill since 2011. It'll happen at some point and will provide more information as to what we should expect purely in terms of litigation liability. That's one vector, and it will settle in the next couple of years.

Another is, "How will technology evolve?" This is one of those secular trends that we're not going to stop. Information security is here to stay. If anything, as Lisa suggested earlier, it's going to permeate more and more of our daily activities. The ways in which hacking or disturbances might occur and who could be liable for it may be spectacularly complex and unpredictable. Many people may be affected by it in the future in ways we can't necessarily foresee today.

The third piece is, "How do businesses organize themselves?" You set yourself up one way today and you might be immune to certain kinds of attacks. To become more efficient tomorrow, you're going to have to reorganize. Some national institutions are doing this. It used to be that their credit card business and their debit retail business and their commercial bank, for example, were all separate. Some of them are considering linking them up a bit more. Now they have to think about their IT environment a lot differently.


Amir-Mokri

PHOTO: DAVE CROSS PHOTOGRAPHY

> "It's incumbent on states that have an interest in the current world order – the U.S., Western Europe, China, Russia, India – to come up with protocols and ways to work with each other to manage this issue."
>
> – Cyrus Amir-Mokri

That's true not just for financial institutions but for any company that wants to use technology to become more efficient. Once you organize yourself in a way to become more efficient, that usually results in different parts speaking to each other. You have to think about your information security architecture differently.

**GILFORD:** Cyrus has perfectly organized the landscape. To expand a bit on the litigation front, litigation is a notoriously unwieldy and time-consuming way to work out policy issues. I don't see that slowing down. As I predicted earlier, we may see a rise in cases at the convergence of product liability and cybersecurity as physical objects in our day-to-day lives are increasingly driven by connection to the Internet and are susceptible to hacking and security threats. I don't see that slowing down. It will result in litigation that will take some time to work its way through the courts.

As I mentioned before, in California, we see an update or amendment to privacy statutes almost yearly that affects all companies doing business in the state. Our clients need to be aware of those changes. For example, California recently legislated the manner in which some companies that provide credit protection services to persons affected by a breach must go about providing those services. If that is something a company decides to do as part of a response plan, it should be aware of jurisdiction-specific requirements.

Those kinds of laws, their meaning and their scope are issues that will be litigated beyond any kind of harm to a particular plaintiff or set of consumers; cases will revolve only around the laws' meaning and application to companies. Oftentimes, the parameters of those aspects of laws get worked out in the courts. It takes time to develop a body of law and an understanding about what the legislative environment is for companies.

The way companies organize themselves and design their products with an eye toward mitigating cybersecurity risks will be an expanding area of focus that will require input by lawyers and others knowledgeable about the legal risks in particular areas.

**LD: Mike, what do you see in the future, particularly from your governmental purview?**

**SCUDDER:** I would make a nonlegal point, which is implicit in what everyone is saying here. If I were sitting with a company, and they were looking into the future — knowing that cybersecurity risks exist today and will tomorrow — I would tell them to double down on their investment in security, both regarding product development and more broadly. Companies should focus on having the right skill set and capacity in their boardrooms and executive suites to deal with these risks, and they should recruit talent that's able to manage this for their institutions going forward. You've got to stay a step ahead. That is the challenge.

**AMIR-MOKRI:** Cybersecurity issues cut across borders. As we think about legislation domestically in the United States, we also should consider working with a number of major international parties, and not just with our partners. I would include China in this broader group because they have a similar stake in maintaining a resilient Internet that is free of malicious attacks.

It's important to develop international standards of conduct. We have a lot of nonstate actors becoming very active in this area. Organizations like ISIS, al-Qaida and others are a real threat to any organized state.

With information security and IT talent growing significantly in many different areas of the world, we shouldn't assume that nonstate actors will be incapable, as they've already shown that they are capable, of causing serious damage. It's incumbent on states that have an interest in the current world order — the U.S., Western Europe, China, Russia, India, etc. — to come up with protocols and ways to work with each other to manage this issue. Protecting cyberspace is our shared responsibility.

**LD: We want to thank all of you for your time. We're excited to be presenting your thoughts on this rapidly evolving area. Cybersecurity risk is real and growing, and it requires vigilance from everyone, including the harried employee clicking too rapidly on an innocuous-seeming link, boards of directors that now need to be cognizant of best practices, companies considering whether and when to self-report an incident, and government bodies responsible for domestic and international standards of conduct for protecting cyberspace.** ■

Skadden

SKADDEN.COM