Technology, Media & Telecommunications

The Metropolitan
Corporate Counsel®

National Edition

www.metrocorpcounsel.com

Volume 23, No. 2

February 2015

Insider's View on Cybersecurity in the TMT Sector

MCC interviews ***David S. Turetsky,*** *a partner at Akin Gump Strauss Hauer & Feld LLP.*

MCC: You bring a unique perspective to the issues facing players in the technology, media & telecommunications (TMT) sector. With government, business and private practice experience, substantive expertise in antitrust, data breach/cybersecurity and other areas, and a view of issues through both the law and policy lenses, you must approach your clients' needs a little differently than most outside counsel. Tell us how you approach issues facing your TMT clients.

Turetsky: One of the things I most enjoy about helping clients is applying the perspective and experience I have from senior roles in government, in business and law firm practice. Having sat in a variety of chairs, I understand the possibilities, needs and limits on the client's side and on the government's side, which really helps me provide the kind of counsel to clients that they value and that can make a difference.

MCC: You have substantial experience at the FCC. Obviously, that relates to the needs and issues that your TMT clients face. Talk about some of the current issues going on and how that experience colors your perspective.

Turetsky: One example is in the area of cybersecurity, which is clearly a serious concern, as many recent events in the news underscore. Having led the FCC's policy area pertaining to cybersecurity – including serving as the FCC's lead representative on White House-led groups focusing on cybersecurity that brought different agencies together and working on projects that brought the public and private sectors together – I've had the opportunity to focus on these issues in a way that not many others have experienced.

David S. Turetsky

At the same time, my business experience makes me sensitive to the importance of business making wise choices with limited resources. Cybersecurity is a particularly tough area because it's emerging. The law isn't settled. Public policy is still being shaped. Attackers have different objectives. There are technical challenges. And the opportunity for business and government to work together in partnerships is not common to all areas.

Cybersecurity was part of my larger reliability, resilience and risk management, and emergency preparedness and national security communications portfolios at the FCC. I worked on the transition to IP networks, Next Generation 911, wireless emergency alerting, wireless 911 caller location, Text-to-911, FirstNet and public safety spectrum issues. I was responsible for leading the FCC's preparation, response and lessons learned from weather-driven emergencies affecting communications, including Hurricanes Sandy and Isaac and a derecho; and other emergencies, such as the hacking of a few broadcasters' emergency broadcast equipment, the Boston Marathon bombing, and the FCC's own continuity of operations program. I also worked on the process for the FCC to obtain executive branch input on national security, law enforcement, trade and foreign policy implications of certain proposed transactions and applications involving foreign investment.

> *Looking at the big picture, the measures we take must be equal to the stakes and risks, which will only increase as more systems and objects get connected to the Internet. Cybersecurity is a vital legal, economic and national security issue. How we handle it will determine how safe we are and our economic future.*

MCC: It seems that government and business stand to learn from one another either in having responded to an issue or in each seeking excellent cybersecurity protections. Do you see the public/private opportunities delivering potential benefits on both sides?

Turetsky: Yes, very much so. It's clear that government is not anywhere close to 100 percent effective in securing even its own information. It's also clear that the vast majority of the critical infrastructure in our

Akin Gump
Strauss Hauer & Feld LLP

Please email the interviewee at dturetsky@akingump.com with questions about this interview.

country is owned and controlled by the private sector, not by the government. So, the private sector needs to play a leading role in providing cybersecurity because it owns the assets that are at risk, and the government doesn't have all the answers. Another implication that some in government understand is that, to meet this challenge, the private sector needs the flexibility and latitude to act, to innovate, to move quickly and adapt to these challenges. That is partly why this has not been, in general, a very rule-bound area.

MCC: What is your assessment of the quality of cybersecurity measures currently in place in the U.S.?

Turetsky: We are not where we need to be as a nation. The threats are real and diverse. They can and do come from nations, criminals, disgruntled employees and hackers. Some companies are taking these threats very seriously and are making good choices about these risks. Some others not as much yet. But even good choices do not guarantee success.

Looking at the big picture, the measures we take must be equal to the stakes and risks, which will only increase as more systems and objects get connected to the Internet. Cybersecurity is a vital legal, economic and national security issue. How we handle it will determine how safe we are and our economic future. We are seeing exciting innovation. But we will not fully realize the jobs, improvements in our lives and other benefits this can bring unless we improve cybersecurity. People need to trust these new technologies, products and services, and for that to happen, cybersecurity will need to be considered and designed in from beginning to end, including every update.

The president and the Congress are clearly focused on cybersecurity, but there is no silver bullet. Some believe that it will take a truly catastrophic event to get the changes needed. I certainly hope that is not the case.

MCC: Let's turn to the private sector. As you said, the threats are real and diverse. Some organizations are making good choices, others bad choices. Parse that out for our readers. How do you advise clients struggling to mitigate these massive financial and reputational risks?

Turetsky: Private companies face very real constraints. The choices they make should reflect the particular risks they face. Those choices need to be supervised by the board of directors. This is not just an IT or legal issue. Nor is the problem unique to companies of a certain size, like Sony or Target: an assistant secretary of Homeland Security recently spoke publicly about being very worried about smaller businesses.

The National Institute of Standards and Technology (NIST) developed a cybersecurity framework as part of the implementation of the president's executive order on cybersecurity. The NIST framework applies across industries and is designed to be a tool to help private companies determine what risks are most important to their businesses and aid them in analyzing how they are addressing these risks and whether there are gaps. It is not a checklist. The risks that get a company's greatest effort may vary depending on what it does. So, a retail company with a lot of personal and financial consumer information has some different risks than a company whose primary business is developing intellectual property and licensing it.

A particular challenge with cybersecurity is the fact that everything is happening so fast. And it's not just that the threats and attacks are evolving. The president has made additional legislative proposals, and Congress says it is going to act. State regulators and enforcers are undertaking new initiatives, and courts are starting to address data breach class actions. The FTC has brought a series of privacy-related enforcement cases and considers, in part, whether reasonable precautions were taken in cases of breach, and the FCC stepped into the data security area with a landmark case last quarter. The SEC has expanded its attention to cybersecurity issues. Regulators are also now connecting through a new group on cybersecurity headed by the Nuclear Regulatory Commission. The NIST cybersecurity framework is getting fleshed out for individual critical infrastructure industries, and as part of that, for example, an FCC advisory group is expected to produce an industrywide report in March dealing with best practices in the telecom industry. NIST also sought comment recently on a draft cybersecurity framework aimed at companies with fewer than 500 employees. There is just so much going on, some of it sector-specific, and companies really need to be aware of a significant amount of it to ensure that they are adjusting to new circumstances and making the best choices.

One important thing a company can do is training. Some don't do that. Nothing will necessarily keep a determined and capable hacker out, but companies should make it hard. Companies can also consider addressing cybersecurity in their supply chain contracts and insurance policies and should prepare and drill a plan and a response team, among several other steps. This issue can go right to a business's reputation and success.

We currently see efforts to segment systems so that getting into one area doesn't get you in everywhere. Encryption is part of that. So is the kind of monitoring that will spot intrusions faster and enable countermeasures to be taken. Enhanced information sharing may help. Yes, hackers will win some of the time. But there's a lot of proactive work underway.

MCC: Given that, what are the key policy considerations corporate law departments in the TMT sector need to keep top of mind as Congress changes leadership and we look ahead to the next presidential election? What legislative and regulatory developments do corporate boards, including chief legal officers, need to be thinking about?

Turetsky: There are some areas where the prospects of getting legislation passed

are reasonably good. One is information sharing about threats and some measure of liability protection for the information that companies share. Another area that will get consideration is a federal standard for notification of breaches. That may enable consumers throughout the country to understand better what protections they're going to get while also addressing the difficulty companies have in coping with different standards in almost all 50 states. Among other legislative possibilities is enhancement of penalties for some of the wrongful conduct we've seen, if the perpetrators are caught.

MCC: Hackers seem to be ahead of the curve in being able to perpetrate their crimes. What efforts are on the horizon in terms of addressing these issues and getting ahead of the hackers?

Turetsky: Different hackers have different abilities and different motivations. They have different targets and objectives. Nowadays it's understood that some hackers will likely succeed in getting into a company's systems. We currently see efforts to segment systems so that getting into one area doesn't get you in everywhere. Encryption is part of that. So is the kind of monitoring that will spot intrusions faster and enable countermeasures to be taken. Enhanced information sharing may help. Yes, hackers will win some of the time. But there's a lot of proactive work underway – I've only mentioned a couple examples – to make that harder.

MCC: We're not reading about those efforts in the news.

Turetsky: Big breaches of confidential information or trade secrets are more newsworthy, and public notifications flag them. Also, companies that have had the most success in maintaining security or at least avoiding bad results don't necessarily want to highlight that for a number of reasons. Nor does success in some fashion one day guarantee success against a different threat another day.

MCC: You have a foot in both a law firm and the public policy group at Akin Gump. Tell us a little bit about giving guidance to clients given your dual law and public policy perspectives.

Turetsky: Many issues are cross-cutting, with statutory or common law aspects, congressional or regulatory angles and the possibility of administrative or court scrutiny or litigation. They have practical and market implications for business. I've litigated class and other actions, been involved in investigations, counseled clients on a wide range of matters, managed businesses, served in-house at a private company where I had to think about and act on a wide range of legal and business issues, and worked on many types of issues with public policy dimensions, inside and outside government, even including disaster and emergency planning and response. It is valuable to understand the law and the political and policy landscape. I very much integrate these perspectives when I look at something like cybersecurity legislation and policy or what a company may or should do in that area, and the same is true in competition and other areas. I sometimes view Washington as an echo chamber, where developments in regulatory agencies, Congress and the courts all affect one another. But I'll be the first one to tell you that, while I have a range of experience in law and policy, I also don't hesitate to reach out to my colleagues in the firm to get expertise that may be relevant and helpful to a client, and I frequently work closely with others here.

MCC: Let's talk about your experience as a senior executive with a telecom start-up. How does that resonate with your TMT clients?

Turetsky: I learned a lot about companies and also about the in-house counsel environment, and that helps. When I left the Department of Justice, I joined a start-up telecom services company. It had about 60 employees. By the time I left it was a public company with about 3,000 employees. I helped to bring it public.

I learned about the rapid pace at which business can – and sometimes needs to – move, the opportunities and risks of technology and the importance of getting things done. I was part of the senior team and interacted with all aspects of the company, from the C-suite to the board, and most areas of the business. As a lawyer, I worked to create a reasonably transparent and business-friendly legal team to help accomplish the company's mission. I was practical and flexible, but at other times, I had to be and was firm. I came to appreciate the significance of the fact that, while outside counsel often deal with in-house lawyers, the in-house counsel's client is often not a lawyer. That puts a premium on both spotting and explaining the legal issues clearly to non-lawyers and helping to assess and address risk. I sometimes say that in-house lawyers need to be able to see around corners, meaning that they have to anticipate the legal issues the company may encounter and try to keep them from becoming obstacles. A very simple example: If the company wanted to sell a certain product at a certain price, there might be regulatory prerequisites in some jurisdictions, such as a tariff filing. It was up to my team to figure that out – what the timetables were, what needed to be done – so that the business would be able to do what it planned at the time it was ready to do it.

I also hired outside counsel, and it was often to obtain more expertise or depth, or some additional ideas or options to help solve or handle a potential problem. Sometimes, it was part of a strategy of managing internal issues, given the different roles and responsibilities within a company. I particularly valued working with outside counsel who were not only expert but also very practical. I try to put that understanding to work now for my clients.

I should add that, when working as a lawyer at a firm, I was appointed twice by federal courts and also by the FCC to be the management trustee for cellular businesses that were required to be divested to preserve competition as a condition of merger consent decrees. I ran all aspects of the businesses for six-month stints until they were sold, and we set sales records in the consumer markets for those businesses. That experience was invaluable and influences how I approach problems now and helped in running the Public Safety and Homeland Security Bureau at the FCC.

MCC: Antitrust issues are top of mind for many TMT companies, a sector experiencing incredible convergence. Where do you see merger review and clearance headed both in the U.S. and internationally as enforcement officials continue to muscle up around the world?

Turetsky: Years ago, there were a limited number of antitrust merger regimes. Today, many countries have them, from the biggest, like China, to some of the smallest. In several jurisdictions, there's a high degree of convergence in the standards that are applied. In others, that is not the

case, and the process and timetable can also be opaque. Some see a certain amount of "home cooking" in the applications of merger law in some jurisdictions. To get a large merger with significant international aspects through involves planning and coordination.

In the U.S., new merger guidelines were adopted a few years back, and experience with them is growing. That doesn't mean the outcome of every deal is predictable. But, as always, the vast majority of transactions continue to proceed to closing without requests for additional information, and most transactions for which additional information is sought also close.

Merger law, like all antitrust law, is highly fact specific. That being said, as most companies understand, deals raising significant horizontal issues are more easily attacked than those that raise only vertical issues. Some contend that too many TMT markets are showing increased concentration, and others point to the evolution and transformation of technology and product markets to argue otherwise. Certainly, for example, music-related markets are obviously very different from years ago. Telephone and television service were once sold by separate companies. The relationship between wireless and wireline service has changed, with approximately 38 percent of households no longer having a wired telephone, not to mention texting, which is moving away from SMS as has been happening in Europe.

MCC: Given recent developments in data security and privacy out of Brussels, is it fair to say the EU is firmly in the driver's seat when it comes to setting the international privacy agenda? Has the U.S. taken a back seat?

Turetsky: Well, the president talked about privacy legislation when he recently appeared at the Federal Trade Commission. I think he was the first president to speak there, possibly ever, but certainly in many, many years. That's a reflection of the importance of the privacy issue in the United States. Congress is interested in those issues as well. States have been very active. I wouldn't describe the U.S. as being in the back seat.

Certainly, in Europe there's a longstanding view of privacy that has different roots than privacy as thought of in the United States, and that can lead to a different approach. There are differences in the cultures and regimes. We see that playing out in the current landscape with such things as the "right to be forgotten" that has emerged from European litigation. But I wouldn't necessarily characterize the Europeans as in the driver's seat, at least vis-à-vis the United States.

MCC: Sounds like it's a matter of priorities.

Turetsky: On both sides of the ocean, and in other places as well, there's a lot of thought being given to what privacy means. Everybody agrees that it is important. Not everybody's coming to the same conclusion about the scope. With different cultures and legal systems, different results may be better suited to different countries. What's important is that a reasonable balance be struck. I don't think these are easy questions.

But this can be very tough on business. They would like consistency and want to be efficient and not have very different and potentially inconsistent requirements in different jurisdictions. There's a lot about this that's challenging.

MCC: If there's is a single bit of free advice you could give to general counsel of TMT companies to help them to rest easier at night, what would that be?

Turetsky: I would advise them to take cybersecurity seriously, make sure it is considered at the board level and press the company to be prepared.

Preparation is vital. Make sure that risks have been assessed and that a team is in place and, apart from other precautions, that your company has a response plan that is tested. You want to avoid a situation in which you are first hiring consultants or lawyers after the breach occurs and introducing them to your business people and systems. Your team should understand the plan and know something about your systems so they are ready to respond.

With these precautions in place, general counsel should rest easier at night.