METROPOLITAN
CORPORATE
COUNSEL®

APRIL 2017 WWW.METROCORPCOUNSEL.COM

SPECIAL SECTION: **CYBERSECURITY**

MCC INTERVIEW: Michael J. Adams / McGuireWoods LLP

Cybersecurity One Step at a Time

The important thing for lawyers is not to get overwhelmed by the complexity

Corporate counsel and their clients, while beginning to appreciate the gravity of cybersecurity challenges, are fatigued by perpetual cybersecurity alarms. ***McGuireWoods*** *partner* ***Michael J. Adams****, who had more than 20 years of experience as a national security adviser in the U.S. Navy, now serves as a strategic cybersecurity and data privacy counselor to clients across industries. He shares his thoughts on transforming reactive corporate culture through the institution of best practices and practical solutions. The interview has been edited for length and style.*

MCC: You initially made your mark in this area through work in the national security space – particularly on the Joint Staff, on the U.S. Pacific Command across the Indo-Asia-Pacific region and, before those assignments, with NATO. You also advised special operations forces. To what extent do those experiences help in advising corporations and corporate counsel?

Adams: My national security experience is incredibly useful to my corporate clients for at least four reasons. In an area of emerging international and domestic legal and regulatory regimes, I have been – and remain – at the forefront of the legal and policy discussions that are shaping the future of law, cybersecurity and data privacy. I am intimately familiar with the technology and the computer scientists and other IT professionals who make it go. Law is constantly lagging behind technology. I help my clients catch up. While not a computer scientist myself, I understand the ones and zeros well enough to translate complex cyberspeak into understandable concepts and sound legal advice. Also the cyber threat vectors are similar, whether directed at private institutions or government systems. We often faced more advanced cybersecurity threats – perhaps the most sophisticated in existence. And finally, I spent much of the past two decades living in dynamic, high-stakes environments. I advised the most senior U.S. government and foreign decision-makers on their most complex and often highly technical operational choices and investments. That skill translates exceedingly well into private practice.

MCC: What is the single greatest cybersecurity challenge for corporate counsel?

Adams: One easy answer is the list of cybersecurity threats, which gets longer and more complex all the time. One might talk about the increasing potency and availability of malware, the professional mobilization of botnets, the magnitude and frequency of insider threats, challenges presented by aging IT architecture and vulnerabilities transferred through merger or acquisition. Another easy answer would be to detail the morass of emerging international, federal and state legal and regulatory schemes and standards that corporations must consider in their day-to-day operations. New York's Cybersecurity Requirements for Financial Services, for example, make the Gramm-Leach-Bliley Act look like child's play. Without constant minding, the legal and regulatory space can feel overwhelming.

However, both the technical and the legal/regulatory space is

manageable – at least with some help. Consequently, the greatest challenge for corporate counsel – and perhaps their most important cybersecurity responsibility – is to work with clients to transform corporate cyber culture from reactive to proactive; from crisis response to practical solutions. They need to help their companies design tailored business solutions, conduct cyber risk assessments, make smart investments, enhance information governance practices and prepare for data breaches – all in advance of true crises.

While cybersecurity is highly technical, managing cybersecurity risk should not be.

Admittedly, this is not an easy task. But in my experience, this is by far the most significant contribution that any corporate adviser can make in this space. And my sense is that this is something that corporate counsel actually want to take on. They are tired of being told repeatedly about nonspecific cybersecurity threats in technocratic lexicon. They feel weighed down by a never-ending cycle of discussions about who did what to whom, how and how much damage was done – all without meaningful, pragmatic advice on what to do about it. To the extent that they see any movement in the field of cybersecurity, they generally think that it is heading in the wrong direction. And their clients feel the same way.

MCC: How can corporate counsel create positive momentum toward change?

Adams: One step at a time. The first step is to stop admiring the problem. Successful business models are forward-thinking, not reactive or driven by crisis. Not surprisingly, successful corporate counsel function in much the same way. Yet corporate leadership and legal counsel tend to get caught up in the technological complexity. They become distracted by the difficulties that many IT and information security professionals have in explaining cybersecurity to them.

But here's the thing: While cybersecurity is highly technical, managing cybersecurity risk should not be. Therefore, the second and most crucial step for building positive momentum is to embrace a series of basic, but tangible, maneuvers. Forget the complexities. Ignore the fact that new legal and regulatory schemes seem to pop up every day. Focus on the task at hand.

Here is some of the practical advice we share with corporate counsel and their clients. Develop and institute a comprehensive cybersecurity strategy. We help clients understand the strengths and weaknesses of their cybersecurity profile by focusing on five areas: risk management and oversight; threat intelligence and collaboration; cybersecurity controls; external dependency management; and incident management and resilience. Our approach is tailored to specific clients and industries, but we always consider the extent to which clients meet certain foundational elements of cybersecurity within these five areas. As an example, we work with banks in their efforts to adopt all the latest guidelines and standards. As industry standards evolve, corporate counsel should ensure that their own strategies are sufficiently comprehensive and that their resources are useful and up-to-date. They should sit down regularly with information technology and security professionals to assess their company's compliance.

Develop and institute a comprehensive information governance policy and supporting procedures. The threshold question that we ask all of our clients is: "Are you in control of your data?" We understand that information is a company's most valuable asset. Yet every company grapples with how to harness, manage and protect that information. It's all about knowing what data you have, where it came from, with whom it can be shared, for what it is used, where it is stored, how it is protected, how long it is kept and how valuable it is. Corporate counsel should be actively engaged in discussions about how to maximize the value of their clients' information while minimizing associated risks and costs. Our experience reveals that a two-pronged approach to information governance is quite effective: Inventory your data and map it for regulatory and legal compliance. That sounds easier than it is. Few lawyers want to be a part of what can be a lengthy and tedious process. Yet the results are invaluable. And if nothing else, corporate counsel should make sure that their clients are following information governance policies, such as data retention schedules, social media policies and legal hold policies, that align with their clients' business models and are both defensible and practical.

Implement a functional incident response plan. There is no worse time to deliberate over complex decisions than in the midst of a crisis. Imagine that you are counsel for a health care provider and that you have worked diligently to comply with HIPAA and equivalent state-specific health care provider rules. You may even have developed specific procedures for responding to disclosures of protected health information. But what if that is the extent of your incident response plan? And what if the next cybersecurity incident at one of your treatment centers has nothing to do with protected information but instead involves an intrusion into the control systems for medical devices? What do you do then? Well, first you panic. Then you might pray. And then (hopefully) you call for help. But in any event, you should have made the time to develop a more comprehensive and functional incident response plan in advance. Whether your corporation retains data in the form of personal information or intellectual property, a detailed but adaptable incident response plan should be in place right now.

Plan with an appreciation for cybersecurity reputational risk. Cybersecurity professionals seem to uniformly agree that government standards can be positive because they have the potential to compel a very basic level of cybersecurity. However, they also agree that few, if any, of these frameworks would actually prevent a professionally orchestrated cyberattack from gaining access to systems, networks or data. To achieve effective cybersecurity, corporations have to exceed minimum industry standards and invest in more – and better – hardware and software. This gap between minimum standards and effective security is the area in which some of the most challenging investment decisions are made. And the stakes are often your company's cybersecurity reputation. I use the term cybersecurity reputational risk to help illustrate a simple reality: In the event of a breach, customers don't care that corporations met minimum industry standards. They care about why the company failed to effectively protect their information. Consequently, corporate counsel and their clients need to consider the possibility that the supposed minimum cybersecurity standards may prove insufficient to meet their fiduciary duties or other obligations to customers.

Focus on the human element. Of the three critical vulnerabilities in cybersecurity – hardware, software and humans – humans present the most significant vulnerability by far. More specifically, insider threats present the greatest likelihood of causing significant cybersecurity incidents. These threats can be deliberate (disgruntled employees) or inadvertent (an unsuspecting person who falls for spear phishing). Studies show that consistent cybersecurity training can produce positive behavioral adjustments, although the precise size of the impact of train-

ing is debated. Still, if employees fall for attacks 20 percent of the time and training reduces that number to 10 percent, it is now half as likely that the corporate counsel will have to deal with the consequences of an employee's cybersecurity error. So train, train and train some more. Furthermore, in focusing on the human element, corporate counsel should also know their own limits. Continue to learn about cybersecurity, data privacy and information governance, but don't be afraid to call on trusted professionals for help.

MCC: Do you have any final advice for corporate counsel?

Adams: Remember, the sky is not falling. It may be filled with emissions and transmissions radiating across frequencies in the electromagnetic spectrum, but it most certainly is not falling. Each day is a new opportunity to push past the weight of cyberphobia, to overcome the threat vectors that try so desperately to push against your corporate and personal goals, and to start building positive momentum through one proactive, practical solution at a time.

Michael J. Adams *is a partner in McGuireWoods' Charlotte, North Carolina, office and a member of the firm's data privacy and security team. He was previously the principal cybersecurity, intelligence, sensitive technical and special operations legal adviser to the chairman of the Joint Chiefs of Staff and a national security point person on cyber threats. A Harvard Law School, Georgetown University Law Center and U.S. Naval Academy graduate, Adams was also deputy general counsel for the U.S. Pacific Command. He can be reached at madams@mcguirewoods.com.*