METROPOLITAN
CORPORATE
COUNSEL®

APRIL 2017

WWW.METROCORPCOUNSEL.COM

SPECIAL SECTION: **CYBERSECURITY**

MCC INTERVIEW: Gus Coldebella and Donna Balaguer / Fish & Richardson

Why Cybersecurity Is Your Board's Business

No company leaders can afford to sit on the sidelines

*For our cybersecurity package this month, Metropolitan Corporate Counsel tapped into the knowledge and experience of two principals at **Fish & Richardson**. **Gus Coldebella** brought with him the regulatory experience of a former acting general counsel of the U.S. Department of Homeland Security. **Donna Balaguer** is a certified information privacy professional who also has in-house experience dealing with the current issues in cybersecurity. The interview was edited for style and length.*

MCC: You have interesting and different backgrounds. How do you work together to help clients protect themselves from cyberattacks?

***Coldebella*:** When I was at DHS, part of my job was helping to lead the legal efforts to improve security of the federal government's computer networks, and to promote robust cyber information sharing between the government and the private sector. In private practice, I do the same for companies, both public and private, that either have experienced apparent cyber incidents or are planning for the inevitable attack. We help clients focus on what should happen before an attack occurs – or, as we like to say, "left of boom." Instituting good corporate governance practices and preparation – not only knowing the enemies and what they might be after, but understanding in advance the regulatory and law enforcement regimes that apply to your company and industry – can help mitigate a disaster.

Balaguer: I help clients take advantage of the incredible business opportunities created and facilitated by technology, while mitigating the risks of cyber attacks and data breaches. I served as in-house counsel in the technology sector and understand the pressures of managing the ever-changing landscape of cybersecurity regulations and best practices while at the same time responding to business needs. Everything is focused on understanding our clients' businesses so that we can evaluate specific risks and opportunities. We then create a comprehensive plan that not only helps the client protect itself in advance, but tells them what to do if an attack occurs.

There are some quick wins that the Trump team can achieve early in the administration.
– Gus Coldebella

MCC: Gus, as the acting general counsel at DHS, you were involved in setting cybersecurity policy at the federal level. Tell us about the potential cybersecurity actions that the new Trump administration may take, and the implications for the private sector.

Coldebella: There are some quick wins that the Trump team can achieve early in the administration. Since private-sector participation in key aspects of cybersecurity – like information sharing – is voluntary, the administration has to find ways to eliminate disincentives to participation, such as the risk of an agency enforcement action after reporting an attack. Companies that are hacked are victims of a crime, and should be treated that way by the government. However, there's a disconnect between the "help-the-victim" and the "blame-the-victim" agencies – a disconnect that the Trump administration should broker.

Also, companies that are compliant with a government-sanctioned standard like the National Institute of Standards and Technology cybersecurity framework, yet are victims of a sophisticated hack, should be afforded some level of liability protection from the government. This is a reasonable approach that both encourages better cybersecurity and recognizes that there is no such thing as perfect security.

MCC: Can you explain why cybersecurity isn't just a server room issue but also a boardroom issue?

Coldebella: It's one of the central enterprise risks that boards of directors and C-suite executives face. Since everything of value is now in digital form – from personal information to credit card numbers, to intellectual property and communications between senior executives about their corporate strategy – bad guys are finding more advanced ways to look at, manipulate and monetize it.

Cybersecurity is, and has to be, a boardroom issue not only because of the potentially devastating primary effects of a successful attack – losing control of one's data or informa-

tion assets – but also because of the secondary effects, which could cause even more significant issues for the company: litigation, regulatory investigations, loss in stock price and the reputational hit that invariably follows. Boards are carrying out this obligation in different ways: establishing special committees to oversee the issue, assigning oversight to the audit committee – even adding "risk" to the committee's name. Experienced outside counsel can help the board create the appropriate tone at the top and document its record of oversight and compliance, both to help it in its stewardship of the company's security, and to protect the company in case the board's actions are reviewed later.

MCC: What steps should companies and their boards do right now to mitigate the risk of a cyberattack?

Coldebella: We urge clients to step back and think about cybersecurity in a strategic way. What are the assets that we have that are valuable? How are we protecting them? How quickly will we know if they're accessed, stolen, deleted or altered? Companies should use a risk-based approach in this analysis: What is most valuable? What is most likely to be targeted? What information assets would be devastating to the company or its customers if unlawfully manipulated?

Once management answers those questions, the board should monitor and oversee the company's cyber work with questions like these: Do we have the right policies, procedures and personnel to make sure that our assets are secured? If an attack were to happen, would the company be resilient – including through implementation of an incident-response plan that has been regularly exercised in mock attacks? Now that the Securities and Exchange Commission has issued guidance suggesting that companies disclose cybersecurity-related risks in their public filings, CEOs, CFOs, general counsel and boards of directors need to focus on whether the company has engaged in a robust process to understand and disclose its cyber risks. This is not a "one and done" board function; since the threat is dynamic, as are the company's systems and information, the analysis and oversight should be ongoing.

MCC: Donna, where do privacy and data security fit into the equation?

We've seen even sophisticated government employees fall for phishing emails that resulted in the loss of very valuable information, as well as public embarrassment.
– Donna Balaguer

Balaguer: It's all about data. Cybersecurity is critical because of the important and sensitive data maintained in cyberspace. Most intruders are looking for data. Companies have their own confidential business data that they obviously want to protect. They may also have collected information from others, such as employees, patients and customers. Companies have additional responsibilities to explain how they will use this outside information and use it appropriately. Companies need to implement data security measures to prevent intruders from getting their hands on it. They must also implement data privacy measures that will govern how they use, share, maintain and destroy the information of others.

MCC: Which business sectors are most vulnerable to cyberattacks and why?

Balaguer: No business sector should feel immune. Any company that holds data is vulnerable, but we can look at which data is the most valuable to an intruder. Financial data is obviously valuable. The financial sector holds this data, but so do companies that collect payment data from consumers. This is why we've seen an increase in attacks on consumer-oriented companies like Home Depot. We've seen a dramatic increase in breaches in the health care sector because of the sensitive data it holds, and those are likely to continue. With the growing internet of things, I expect to see more breaches in the manufacturing industry as well.

MCC: What are five questions every CEO should ask about cybersecurity?

Balaguer: Who are the employees in charge of cybersecurity at our company? What are our cybersecurity risks? What are our policies and procedures to manage those risks? How do we manage related risks, such as data privacy? And how do we ensure that our policies and procedures are followed companywide?

MCC: What types of claims can result after a cyber breach, and who can sue?

Coldebella: We have seen cases involving allegations of personally identifiable information being lost in an attack. For public companies, plaintiffs have brought 10b-5 stock-drop cases – securities fraud actions that allege that the company's public disclosures did not tell the whole truth about the state of its cybersecurity risk. We've also seen – and this is of particular interest to corporate directors – claims for breach of fiduciary duty, alleging that a board of directors ignored the red flags of this type of attack potentially happening.

The other area is regulatory investigations. The FTC has been the big dog in the junkyard, bringing cybersecurity actions against companies that have experienced attacks. But the SEC is also beginning to flex its cyber muscles. The SEC has regulatory authority over public companies' disclosure obligations, and it's been using that authority with increased vigor to try to raise the cybersecurity game of those companies that are within its regulatory ambit. I imagine that, soon enough, if the SEC Enforcement Division believes that a hacked company's cybersecurity disclosures were subpar, it will test its enforcement powers against that company.

MCC: Donna, can you explain why cybersecurity is an issue that needs buy-in from every employee in a company?

Balaguer: You can have the best cybersecurity intentions and practices, but they won't mean anything unless the entire company is on board. Employees are critical to cybersecurity. We've seen even sophisticated government employees fall for phishing emails that resulted in the loss of very valuable information, as well as public embarrassment. Intruders will look for the weakest link, so cybersecurity must be instilled throughout the company.

MCC: How can companies instill a corporate culture of compliance?

Balaguer: The culture must flow down from the top. The company executives must make it clear that cybersecurity is an important company value and is part of the company's core identity. In terms of training, cybersecurity is not a once-a-year issue. Engage in ongoing interactions with employees about cybersecurity, including telling them about the newest devious methods that hackers are using. Make the training engaging and maybe even fun with drills and exercises. Don't take a one-size-fits-all approach; instead, tailor training according to employees' job responsibilities. The bottom line is that cybersecurity awareness should be made a routine part of every employee's workday.

Gus Coldebella *is a principal at Fish & Richardson, where he focuses his practice on helping companies deal with all aspects of cybersecurity incident response and planning, government and internal investigations, complex civil litigation and crisis management. He previously served as the acting general counsel of the U.S. Department of Homeland Security. He is based in Fish's Boston and Washington, D.C., offices and can be reached at coldebella@fr.com.*

Donna Balaguer *is a principal at Fish & Richardson, where she focuses on advising clients on cybersecurity and data privacy laws and best practices, from the early stages of developing an internal framework to handling a cyberbreach. She previously served as an executive and in-house counsel to both entrepreneurial and major corporations, and advises a wide range of clients in the hospitality, health care, publishing, communications, manufacturing and retail industries. She is based in Fish's Washington, D.C., office and can be reached at balaguer@fr.com.*