EXTERNAL TECHNOLOGICAL VENDORS ASSISTING IN REGULATORY CHANGES

BY **JASON PILL,** EMPLOYMENT DEFENSE ANDCYBERSECURITY ATTORNEY AT PHELPS DUNBAR

What are your roles and responsibilities in your organization?

Currently, I serve as an employment defense and cybersecurity attorney. My daily practice consists of a mix of employment law and cybersecurity law. Primarily, I work with employers on all levels of workplace issues, including harassment, discrimination, and other disputes that may arise in the workplace. As a part of that I work with companies to protect their digital assets and their corporate information, trade secrets, etc.


JASON PILL

We achieve this through a variety of means, including restrictive covenant agreements and other things that govern the employee's behavior, but we also advise on technological ways to protect their assets.

In addition to my employment practice, I also do a good bit of work defending breached companies and litigating class actions filed against companies that have been the victims of a data breach in state and federal court.

What are some of the major challenges and trends currently impacting the cybersecurity industry?

The main challenge we see from the cybersecurity side is compliance, since there's an ever-evolving series of laws across the country, mainly at the state level and federal laws. Different protocols in industries are required, such as regulating data protection standards, notice requirements, and other protocols.

Compliance has become a critical concern for companies, which want to make sure that they are complying with state and federal laws. And as a corollary, it also makes sure that they are protecting their data from data breach incidents. Clients are now not only concerned about compliance, but they are also taking precautions to avoid a data breach and are in the best position to defend themselves against inevitable class action lawsuits.

Could you explain some of the trends happening in the cybersecurity space today and where you think the industry is going?

There is an increased regulatory effort, both in terms of enacting additional laws and restrictions. We are seeing a lot more efforts at the state level and the federal level to enact additional legislation and obligations on companies about how they store, personal data.

The other thing that we see in the private sector is increased litigation involving individuals whose information was compromised as part of a data breach. In the last 10 years, there have been significant strides in that space as the jurisdictional landscape evolves and changes. Because of the massive influx of filings related to these data breaches, we now have courts that are trying to grapple with theories of recovery that fit into traditional legal principles and traditional torts.

So now the question is: how do we fit into these existing regimes? How do we fit these new modern harms into pre-existing notions of duty under a negligence theory or a contract claim?One thing that is changing in the legal world is that more courts are attempting to apply these principles to data breach cases in order to determine when someone has been harmed enough to bring a claim in court.

There have been a massive number of judicial opinions issued on this topic. Specifically, on this topic of standing, more clarity is emerging, although it remains a fluid issue and some jurisdictional issues depend on where the case was filed.

We are seeing the next evolution beyond standing and figuring things out; now we're seeing more challenges towards causation, a suit that means the plaintiff must prove that her injury is linked to the defendant's conduct. A defendant will not be liable to a plaintiff if the defendant was not the cause of the plaintiff's injury, even if the conduct was extremely negligent.

As we have more and more data breaches going on in our daily lives, it becomes harder to trace any alleged harm to any specific data breach. For example, if you were the victim of three data breaches last year and you got three notice letters in your mailbox saying that your phone carrier had breached your banking company and maybe an online retailer you used had been breached, what would you do? And how would you be able to trace any type of potential identity theft or compromise of your personal data back to any of those three breaches? That's a challenge that courts are now looking at with more intensity and scrutiny, as we have kind of progressed in the legal setting by looking at these standing issues. The question is, how do we show that somebody's data was compromised in a specific region? Those are the main areas in which things are evolving.

Increased regulatory involvement in terms of new laws and statutes being enacted and increased regulatory enforcement from the state and federal agencies that regulate and police those laws. The lawsuits have been happening for quite a while, but we expect to see even more being filed on larger levels, with larger class sizes, and more jurisprudence developing as more cases get ruled upon that will hopefully better define the contours of those lawsuits.

What advice would you give to your peers and those aspiring in the digital cybersecurity space?

What would you recommend are the necessary steps they need to take to navigate the growing complexities, be it within the legal space as well as in their organizations as well?

For companies that are trying to figure out where to start, they need to consider not just their internal resources but external resources as well. If there is any type of abnormal activity or misconduct detected, they need to make sure that they're prepared to move swiftly with a cyber-attack protocol. This will enable them to know immediately in the event of an incident.

The companies need to explore external resources, for instance, by working with technological vendors who help assess their systems. The team can be fully embedded within the organization but often requires external assistance because no one individual can keep up with all the regulatory changes.

My strongest piece of advice would be to fully embrace a team mentality in your cyber methods and protections to make sure that the company is looking at all angles and taking a comprehensive approach that's going to provide the best support and security.

And then likewise, for any individuals who are looking to do this type of work from a legal perspective. There's no way to fast-track it; you must familiarize yourself with the statutes if you're looking to do privacy counseling, data privacy counseling, or cybersecurity counseling. There are several significant and complex statutes that sometimes overlap.

> "SUPPLY AND IMPLANT CHARTING IS A CRUCIAL PART OF THE OVERALL PATIENT RECORD AND OF REVENUE GENERATION IN MOST HOSPITALS, AND ERRORS CAN HAVE QUALITY AND REIMBURSEMENT IMPLICATIONS"

It could be a very demanding practice to keep up with everything. If you're trying to do more work in the data breach space, getting experience with class actions under federal Rule 23 of Civil Procedure and corresponding state laws is the best thing to do.

Besides that, there are burgeoning questions of causation and damages, quantifying those damages, and proving that they're connected to a particular breach. Those are emerging issues that will continue to be litigated and will likely have years and years of decisions in the future trying to add clarity. So, having a strong litigation foundation of class actions, we're best suited to defend companies that have experienced a cyberattack.CA