LATHAM & WATKINS LLP

DISCUSSING THE TRENDS

Q&A with Latham & Watkins partners Jennifer Archie, Gail Crawford and David Schindler

The General Counsel's Role Before and After a Data Breach Incident

October 6, 2014

"It is often said that there are two kinds of companies out there — those that have suffered a data breach and those that will have one," said Latham & Watkins partner Kevin Boyle. "So it makes a lot of sense to be prepared in advance."

Today, lawyers for large enterprises must assess and advise on complex multi-jurisdictional notification, investigation, litigation and remedial issues that arise following a major data security incident. Incidents range from unauthorized network intrusions with unknown impact, to massive disruption or denial of the availability or integrity of data, to large-scale theft of corporate trade secrets or consumer data.

In this lw.com interview, Latham partners Jennifer Archie, Gail Crawford and David Schindler discuss best practices for general counsel when responding to the broad spectrum of cyber intrusions that can threaten a company's most sensitive information — particularly where diverse laws protect data sets, and potentially conflicting legal standards govern a company's ability and obligation to respond.

How has the role of the legal advisor changed?

Archie: The legal risks associated with data security are growing exponentially. The legal advisor's role must not be marginalized; it should be front and center in terms of project management. When a data breach occurs, contracts with customers and vendors have often allocated that liability. Written agreements may also impose expectations — explicitly or implicitly — as to how the incident will be handled and how the financial consequences of the incident, both direct and indirect, will be allocated up and down the chain of affected parties.

Schindler: One of the things that's often hardest for general counsel is trying to deal with all the moving parts. Historically, data has been the province of IT. But as you start thinking about things like a company's crown jewels — whether it's actual customer data or the secret sauce you developed — the US Securities and Exchange Commission, your board of directors and others are particularly invested in the extent to which the company is not only protecting those things but addressing risks associated with potential breaches. And as you start dealing with potential breaches, you also have to think about what you need to do in anticipation of the legal proceedings that often follow on the heels of these breaches.

What kinds of threats and risks do companies need to prepare for?

Archie: Inside the company you can have malicious actors who have exceeded the expected parameters of their privileges; these are privileged individuals who have been trusted with access and misused the trust, for example, by passing trade secrets to a competitor.

Many breach notifications and resulting consequences arise from mislaid documents, laptops, removable media and mistakes that happen while administering expected IT functions, such as changing out a server. Hackers can be in the headlines but your legal headaches will more likely arise from mislaid or mishandled data — the loss of privacy, confidentiality, integrity or availability of those documents can be deemed a very significant issue.

Schindler: Traditionally we talk about advanced persistent threats (APT) and state-sponsored espionage at the US Department of Defense or a nuclear power plant. But more and more what you have is foreign governments taking over the networks of the most benign companies to gather information. A pretty diverse universe of foreign governments, pirates and others are looking to launch attacks — they are sitting in your networks and taking over your networks so the networks can be available down the road. This is something that most general counsel don't think about and yet that's what we are seeing more often.

Crawford: APTs are increasingly becoming interested in financial and market data. That's a bit different from stealing plans for the latest fighter aircraft. The malicious actors want to put themselves in a better position in terms of M&A activity and opening up in new jurisdictions. This is a step change in terms of the types of organizations that need to think about this sort of attack and whether or not they are a highly attractive target.

How can companies insure against a data breach?

Crawford: If you don't know what your cyber insurance policy says or what your position is, you need to check it out now. In particular, understanding whether you have cover, and if you do, what the excess is, what direct costs are covered in terms of restoring network security, investigating the attack and obtaining legal advice on notification and data protection issues. Cyber insurance is a market that's going to develop very quickly over the next few years and you need to know where you stand and be looking at it proactively.

For More Information

Latham partners Jennifer Archie, Kevin Boyle, Gail Crawford and David Schindler participated in a webcast entitled "Data Breach Incidents: The Role of General Counsel Before and After." This pre-recorded webcast will be available until December 22, 2014 at 10:30 AM Pacific Standard Time.

Additionally, Latham partners Peter Rosen and Bob Steinberg, and associates Margrethe Kearney, Martha O'Connor and Neil Rubin authored a client alert entitled "Cyber Insurance: A Last Line of Defense When Technology Fails." The alert evaluates the purchase of a cyber-liability insurance policy, an important method of managing cyber risk.

CONTACTS

Jennifer Archie
Washington, D.C.
T +1.202.637.2205
jennifer.archie@lw.com

Gail Crawford
London
T +44.20.7710.3001
gail.crawford@lw.com

David Schindler
Los Angeles
T +1.213.891.8415
david.schindler@lw.com