Why you need a cyber attorney

By **ethicalboardroom** -

By Shawn E. Tuma – Cybersecurity & Data Privacy Partner, Scheef & Stone

Companies are beginning to understand that cyber is an overall business risk, not just a technical issue. Now they must realise that cyber is also a legal issue. The easiest way to understand why is to ask these two questions: 'Why do we know about the data breaches of Target, Yahoo, Equifax and all the others?' and 'Did those companies air their dirty laundry just because they believed it was the right thing to do?'

Of course not! They did so because laws and regulations made them. Those laws and regulations require companies to disclose their breaches and mandate things, such as who they must notify, when and how they must notify, what must be communicated and what must be done for those who were impacted. As these rules demonstrate, having data creates risk and one of legal counsel's roles is to help companies manage that risk.

Many attorneys explain their primary value through their wielding of the attorney-client privilege, by helping to cloak the cyber risk management process with the attorney-client privilege. While that can be helpful when done correctly, it is greatly underselling the real value that experienced legal counsel can add. When it comes to managing cyber risk, there is no substitute for experienced legal counsel.

Real world experience for assessing and managing risk

To effectively manage cyber risk, companies must understand what their real cyber risk is because they cannot manage that which they do not know or understand. The process of assessing a company's overall cyber risk is one of the most crucial steps in the risk management process. It is the foundation.

Attorneys who have substantial experience in dealing with cyber risk are able to better understand how to manage cyber risk, including legal and regulatory liability that leads to significant risk in this environment. Think about this: how many cyber incidents or data breaches has your company's information technology, security and management teams been through or even observed first hand?

Counsel with many years of experience serving as a 'breach guide' or 'breach quarterback,' leading companies through the cyber incident and data breach response process, will have been involved in hundreds or thousands of cyber incidents and data breaches. This real-world experience is invaluable for helping companies understand the real-world risks they now face. Without such practical experience, companies are more likely to spend their resources chasing some of the hyped-up threats that make the best sales pitches, conference talks and news headlines – it isn't always the most exotic and sophisticated attacks that cause the most problems.

Diving deeper, such counsel will have a unique perspective on the most common attack tactics that have been used in the past and that are currently being used against certain types and sizes of companies, in certain industries, with certain types of data and business models and in certain markets. They will also understand the types of attacks that are most likely to lead to reportable data breaches. They will have a better understanding of the laws and regulations applicable to the jurisdictions in which the companies operate and what they require in terms of securing information, disclosing breaches of such information and the all-important question of distinguishing between a non-reportable incident and a reportable data breach, a subtle yet bet-the-company distinction.

"ATTORNEYS WHO HAVE SUBSTANTIAL EXPERIENCE IN DEALING WITH CYBER RISK ARE ABLE TO BETTER UNDERSTAND HOW TO MANAGE CYBER RISK, INCLUDING LEGAL AND REGULATORY LIABILITY THAT LEADS TO SIGNIFICANT RISK IN THIS ENVIRONMENT"

Deeper still, by calling on their history of cases, they will have a unique understanding of those things that companies did right and those things that were ineffective or led to problems. Because no two are alike, this insight provides a deeper understanding of what caused many cyber incidents, how they happened and what could have prevented them. Once an incident has occurred, the focus shifts to an understanding of what companies did right or wrong, or could have done but did not do, that may have improved the response and better mitigated the situation. Finally, it enables them to uniquely understand the true harm to companies that such cyber incidents cause, from the initial panic, administrative burden and confusion and disruption of operations, to the loss of business opportunities due to the companies being focussed on the incident, to the better-known harms, such as the costs of remediation and incident response, negative publicity and the decrease in business value and stock prices.

When working with companies on their cyber risk management programmes, one of the most frequently asked questions is, 'how do you prioritise the steps in your strategic action plan?'. Because companies can't 'boil the ocean' (i.e. fix every problem) and companies do not have unlimited resources to throw at this problem. They must be able to evaluate the risks and develop a strategic action plan that prioritises those things that should be done first. There is a lot more to consider than the traditional risk formula of 'risk = probability x loss' because there are important business factors that must be considered. When evaluating how to prioritise the actions to take, the analysis translates into something more akin to 'risk = probability x loss x

time to implement x impact on the business and resources x benefits/hindrance.' To work through an analysis such as this requires not only drawing on real-world experience to understand the most likely risks companies face, but also requires having an understanding of the overall business, its operational needs, the practicalities of the business environment and the many competing interests that must be considered. Analysis of such complexities is an essential skill for legal counsel.

With cyber risk, even the most extensive and effective risk management programmes cannot come with guarantees. The problem is not a static problem that can be solved, rather, it involves an active adversary that is continuously evolving its strategy and tactics to find more effective ways of attacking and exploiting its intended victims. And, as with security in general, the company must get it right 100 per cent of the time and the attacker needs only one lucky shot. Because of this, when it comes to legal and regulatory liability, the question is usually not as simple as 'did the company have a data breach?' but is more like 'before the company had the data breach, was it taking reasonable measures to protect its network and data to keep from having a data breach?' Well-documented evidence of its diligence can go a long way.

Privilege is valuable, but it must be done right

Not to be ignored, the attorney-client privilege can play an important role in many jurisdictions, such as the United States. However, because the privilege applies to communications and does not shield facts, it is not as effective or certain as many think for either pre-incident risk management or post-incident response.

The best way to help ensure the privilege applies is to have the activities integrally intertwined with the rendering of legal advice by ensuring the attorney is retained first, then the attorney retains and directs the work of consultants and that attorney's role is prominent by truly leading the process so that the consultants are reporting to the attorney who is then using their work to render legal advice. Even then, however, there are no guarantees with privilege. The best course of action is to prepare by doing everything possible to have the privilege but carry out the work as though there will be no privilege because there may not be.

There is no substitute for experienced legal counsel in managing cyber risk. In today's business environment, cyber is unquestionably a legal issue and experienced legal counsel must be integrally involved in helping companies manage their cyber risk.

About the Author:

Shawn Tuma (@shawnetuma) is a cybersecurity lawyer business leaders trust to help solve problems with cutting-edge issues involving cybersecurity, data privacy, computer fraud and intellectual property law. Shawn is a frequent author and speaker on these issues and has used social media to help build his practice. He is a partner at Scheef & Stone, LLP, a full service commercial law firm in Texas that represents businesses of all sizes throughout the United States and, through its Mackrell International network, throughout the world.

Also available as part of the eCourse
2022 Nonprofit Organizations eConference

First appeared as part of the conference materials for the
39th Annual Nonprofit Organizations Institute session
"(2:25 p.m.) MASTER CLASS: Data Protection and Cybersecurity"