New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 257—NO. 43
TUESDAY, MARCH 7, 2017

Outside Counsel

Expert Analysis

Cybersecurity and Due Care For Law Firms

By **Chris Moschovitis**

On Dec. 12, 2016, the American Bar Association's Journal ran a story by Debra Cassens Weiss titled "Unsealed suit targets law firm for alleged lax cybersecurity." It reported on the recently unsealed complaint against a Chicago law firm alleging that they put client information at risk because of poor cybersecurity practices. This news does not come as a surprise to any cybersecurity professional.

On the contrary, we have seen this time and again, and across the range of responsibilities. Owners, and law partners, although "sensitized" to cybersecurity issues, frequently abdicate their due care responsibilities when it comes to cybersecurity, preferring instead to depend on their technology departments to "make the problem go away." This is a clear violation of due care, and a wide-open door to lawsuits.

Roles and Accountability

To understand why this is the case, one needs to recognize the difference between the cybersecurity function and the IT function. In the simplest terms possible: IT creates value. Cybersecurity protects value. Understanding this simple fact quickly demonstrates why cybersecurity cannot, and should never, report to IT. You're asking the fox to guard the henhouse. Think of it this way: Would you have your own accounting department be responsible for auditing itself? They'd pass the audit every single time!

To make things worse, there is a fundamental disconnect in understanding one's role in risk management. Again, in the simplest of terms, consider: Who is responsible for accepting organizational risk? The answer is always the senior partners or firm owners. It is they who accept risk and communicate this to the management team. It is always the partners or owners who must accept risk. If they do not, their inaction becomes a violation of due care.

> Engage with diversity. Surround yourself with trusted advisors that represent different areas of the firm's business and give them an equal voice.

CHRIS MOSCHOVITIS *is the chief executive of tmg-emedia and co-author of "History of the Internet: 1843 to the Present." Chris is working on his latest book "Cybersecurity Program Development for Business: The Essential Planning Guide" to be published by Wiley later this year. He can be reached at Chris.Moschovitis@tmg-emedia.com*

The management team, and the cybersecurity function in particular, is there to advise and frame the cybersecurity risk in a language and terms that the owners or partners can understand, and then they decide what risk to accept, what risk to transfer (e.g. insurance), and what risk to mitigate through the use of controls, who must be deployed via a well thought-out defense-in-depth strategy specific to each business. Moreover, cybersecurity is not static, anymore than IT is. Technologies change, threats change, business assets go through life cycles (what was "top secret" yesterday is "public domain" today), workflows change, and of course people change. Cybersecurity, therefore, must keep pace with the changes.

Operationalizing cybersecurity, just like operationalizing IT, is not trivial. You need to depend on experts to deliver and support the right technologies and solutions for your organization. Depending on company size and business scope, you can chose to have both IT and cybersecurity departments in-house, or outsource them, partially or whole. The critical thing to always keep in mind when it comes to cybersecurity is this: You can outsource the responsibility, but you can never outsource the accountability. You, the owners or partners of the firm remain accountable for exercising due care. If client matters fall into the wrong hands because your cybersecurity vendor, or department, failed to protect them, you're on the hook. Not them.

Going Forward

Where does all this leave you?

First, recognize your place in the risk food chain, and own it. Second, as distasteful a distraction from your "core business" it may be, you need to educate yourself enough so you can make appropriate due care decisions. The time of isolating cybersecurity or IT and relegating it to "the techs" is over. Today, both cybersecurity and IT are "core business."

Finally, engage with diversity. Surround yourself with trusted advisors that represent different areas of the firm's business and give them an equal voice. Learn what matters to them and what's important to them that warrants protecting. The "mission critical" asset in the finance department is not necessarily the same as it is in business development, or operations. This will help you avoid making decisions based on your own bias of "what's important." If you're responsible for due care, your care should extend to the whole organization, not to your favorite (or comfortable) area.

Recognizing the problem is the first step in resolving it. Taking these steps will ensure that you have exercised your due care responsibilities appropriately and completely. At the end of the day, that is the only thing protecting you from negligence.

Reprinted with permission from the March 7, 2017 edition of the NEW YORK LAW JOURNAL © 2017 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 070-04-17-29