Jul 10, 2019

Categories:

Technology Blog

A Primer for Litigation Counsel Regarding the Organizing of Loan Workout and Cybersecurity Professionals

Substantive Expertise versus A New Perspective and Freedom from the Past

Counsel are regularly and appropriately warned against actual and apparent conflicts of interest. This often means that experience with a matter must be abandoned when a "fresh set of eyes" owned by a previously uninvolved lawyer or law firm replaces counsel who was involved in a particular contract or litigation matter. The legal profession acknowledges that avoiding real and apparent conflicts can have costs, but the benefit is understood to outweigh those costs.

The concept that a fresh perspective and independence have value is not unique to practicing lawyers. Neither is the thought that prior involvement in a situation or with the persons involved in a particular situation might prevent a professional from acting objectively. Even though a doctor may have more experience with her own family than any other medical professional, we all know that doctors are counseled against treating their family members. See the AMA Code of Medical Ethics Opinion 8.19 titled *Self-Treatment or Treatment of Immediate Family Members*.

Litigation counsel who represent financial institutions recognize this same dynamic in lender clients who transfer management of a troubled lending relationship to an employee different from the one that initiated the relationship – in fact, in larger institutions the transfer of responsibility for management of a loan relationship may occur twice: (i) first from the originating loan officer to a "relationship manager" who administers the loan in the ordinary course; and (ii) there is often a second transfer of management of the borrower relationship from the "relationship manager" to a troubled loan specialist if the loan becomes nonperforming or under-collateralized. Beyond just changing employees responsible for a lending relationship, in larger financial institutions, the troubled loan management experts are commonly segregated from the other

FBT Gibbons

loan generation and relationship management employees into a "special asset" or similarly named department with a separate management structure. These intra-bank transfers between employees sacrifice personal relationships, historical knowledge, and experiences between the employee losing the file and the borrower in favor of loan management by a new employee with the proverbial "fresh set of eyes" and who (presumably) has no relationship with the borrower that might cloud objectivity.

The above-discussed concepts have found their way into the management structure of financial institutions' cybersecurity professionals. Cybersecurity professionals are technology and computer experts whose focus is different from, but related to, a companies' computer and information systems professionals. Despite the fact that they are not responsible for the operation of a companies' technology and information systems, cybersecurity professionals must be intimately familiar with those systems so they can assess vulnerabilities and know the most likely avenues for attacks by outside hackers or disgruntled insiders. The need for familiarity would seem to argue for a management structure that groups cybersecurity professionals together with other technology and information systems professionals. For financial institutions, that argument is losing in favor of the same concerns about lack of independence and objectivity that have prevailed in the other situations mentioned above. This management separation structure is supported by regulators. *See* https://ithandbook.ffiec.gov/it-booklets/information-security/i-governance-of-the-information-security-program/ib-responsibility-and-accountability.aspx which includes this:

To ensure appropriate segregation of duties, the information security officers should be independent of the IT operations staff and should not report to IT operations management. Information security officers should be responsible for responding to security events by ordering emergency actions to protect the institution and its customers from imminent loss of information; managing the negative effects on the confidentiality, integrity, availability, or value of information; and minimizing the disruption or degradation of critical services.

Separation of cybersecurity professionals from other technology-focused employees is a popular topic among commentators too. *See* https://www.securityroundtable.org/whats-the-best-reporting-structure-for-the-ciso/ which included this in April 2018:

… the question of whom the CISO should report to has likewise risen in importance. Historically, the CISO reported to the CIO, but companies are increasingly considering a number of alternatives—from placing the CISO in the risk or enterprise data groups to having them report directly to the CEO or the board.

Even if cybersecurity professionals are structurally separate from other information technology professionals, those cybersecurity professionals must have access to all the information that operations related technology professionals possess[1] so that danger can be assessed and defenses (and interventions because problems will occur) can be designed and implemented. When a company's organizational structure removes cybersecurity professionals from other information technology professionals, extra efforts must be made to ensure that the cybersecurity professionals have the necessary information.

As hinted above, cyber security professionals corporate reporting structure varies within organizations. Personally, I believe that organizing cybersecurity professionals with other risk management professionals is a very good option because in all cases these employees: (a) must work with other employees to locate and deter internal losses; (b) anticipate and block losses caused by outsiders; (c) do all this work while balancing risks with the costs in time, money and aggravation imposed on the organization by risk reduction efforts; and (d) be prepared to work with outside counsel when problems arise.

What does all this mean for litigation counsel representing financial institutions? I discussed previously the need for litigation counsel to understand a client's information management systems to ensure that required information is gathered from all appropriate files and sources. *See* *What a Collection Lawyer Should Know About a Client's Information Management Systems* (10/22/18).[2] The separation of cybersecurity professionals from your client's information technology staff increases the need to understand the

client's information management structure and ask the questions discussed in that prior post. This is true, in part, because cyber professionals will have made vulnerability assessments and implementations of suggestions from cybersecurity professionals will have (hopefully) influenced the operation of the information management system.[3]

For a financial institution's counsel, the separation of cybersecurity professionals from your client's information technology staff has implications beyond the work required to respond to discovery and prepare your case. The need to involve both technology professionals and cybersecurity professionals is obvious if your litigation involves alleged breaches of the client's cyber security. But, that is not the only situation where litigation counsel need to understand the distinction being discussed herein. Consider these real-life examples:

- In litigation alleging theft of a borrower's business idea disclosed in the loan application process, litigation counsel worked to show that the client's internal controls on information availability prevented the employee whose relatives opened a competing franchise from viewing the loan application;
- In litigation alleging discrimination, litigation counsel worked to show that the client's underwriting decision maker who considered the collateral did not have access to the demographic information at issue; and
- Cybersecurity professionals provided valuable expertise helping to show that unauthorized access to a customer's account came from the outside and not problems with the client's ATM machine.

In sum, separation of cybersecurity professionals within an organization from other technology professionals provides significant benefits including the acknowledged benefits arising from the concepts of separation of duties, avoidance of conflicts of interest, and a fresh perspective. Counsel need to use these benefits by recognizing and using the different perspective and expertise made available by these employees who often are not

part of traditional financial institution litigation. And, when litigation involves issues directly impacting these professionals, counsel need to understand and handle (emphasize, harmonize or minimize as appropriate[4]) the different emphasis within your company's various departments.

Vince Mauer has a master's degree in Business Administration and passed the CPA exam. Licensed in Ohio and Iowa, he has represented financial institutions in litigation matters for over 30 years. For more information on this topic, contact Vince Mauer at vmauer@fbtlaw.com.

---

[1] This includes the structure of information generation and storage, who can access the same internally, external access by business partners like account holders and others (website visitors). The information system operated by information technology professionals must limit what information can be accessed based on who seeks the data and cybersecurity professionals must ensure that those barriers are not breached.

[2] *See also* The Commercial Litigator and His Client's Information Management Systems (10/11/18). https://www.fbttechblog.com/the-commercial-litigator-and-his-clients-information-management-system.

[3] Separation of cybersecurity professionals from the operation of the company's technology process is another example of the well know Separation of Duties ("SOD") requirement that forms a fundamental basis of a company's internal accounting controls. Financial auditors measure how a company implements SOD in its operations and that includes technology aspects of the company's operations. *See* https://www.aicpa.org/interestareas/informationtechnology/resources/value-strategy-through-segregation-of-duties.html. For a similar thought involving lawyers, consider the prohibition on lawyers serving as witnesses and advocates in the same proceeding set forth in Rule 3.7 of the ABA Model Rules of Professional Conduct. Just as a lawyer should not serve as an advocate in a case when he is a witness to the events at issue in a trial, so an IT professional should not evaluate and be solely responsible for the security of a system she

designed.

[4] For example, in litigation that private financial information was wrongfully disclosed to a co-obligor, the cybersecurity professional who did not design or implement the information management system that permitted the disclosure to occur was permitted to provide quasi-independent expert testimony that the information management system was typical of such systems in use by financial institutions.

FBT Gibbons