UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

The University of Texas School of Law
33rd Annual School Law Conference

February 22-23, 2018

Austin, TX

Cybersecurity Planning

Leslie C. Thorne
Emily Westridge Black
Haynes and Boone, LLP / Austin, Texas

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Other Authorities

Introduction

Major data breaches are making headlines on a near-weekly basis—from the more than 75,000 ransomware attacks in over 99 countries on May 12, 2017 to the Equifax hack which led to the personal data of 145 million people being stolen. These attacks are increasing in size and frequency for a number of reasons, including because companies and individuals' confidential data is valuable to hackers. Law, accounting, and financial firms have traditionally been high-value targets because they hold a large amount of sensitive client data. But schools and colleges are increasingly becoming hot targets for hackers for the same reason: they are repositories for sensitive personal data. To mitigate the risk and effect of cyber attacks, schools should take steps to prevent data breaches and mitigate the damage if one does occur. Because financial institutions and regulatory agencies have been on the forefront of cybersecurity, the models and guidelines provided in that sector are helpful to any institution looking to develop or bolster its cybersecurity planning.

Ethical Obligations

Firms and schools that maintain confidential client data should establish effective cybersecurity policies because it is good for business and to comply with the ethical rules for attorneys, which generally prohibit the disclosure of client information to third parties.

The American Model Rules for Professional Conduct ("ABA Model Rules") set standards for ethical behavior within the legal profession. *See* MODEL RULES OF PROF'L CONDUCT. One focus of the ABA Model Rules is protecting the confidentiality of client information. *See* MODEL RULES OF PROF'L CONDUCT 1.6. Under ABA Model Rule 1.6, "a lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." *Id.* Comment 18 to Rule 1.6 provides that "reasonable efforts" are determined by looking at several factors: (1) sensitivity of the information, (2) likelihood of disclosure if additional safeguards are not employed, (3) cost of employing additional safeguards, (4) difficulty of implementing the safeguards, and (5) extent to which the safeguards adversely affect the lawyer's ability to represent clients. MODEL RULES OF PROF'L CONDUCT 1.6 cmt. 18. Given the sophistication of hackers and their documented interest in attacking client-service firms that maintain large volumes of sensitive information, law firms should comply with this rule by carefully assessing the sensitivity of the client information they maintain (including, *e.g.*, personal information of individual clients and sensitive business information of corporate clients) and determining how to effectively protect it.

When considering how to protect client information, lawyers should be aware that the ABA Model Rules also require practitioners to stay current with changing technology. ABA Model Rule 1.1 provides that "[a] lawyer shall provide competent representation to a client … [which] requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." MODEL RULES OF PROF'L CONDUCT 1.1. Comment 8 to Rule 1.1 elaborates on this duty:

> [A] lawyer should keep abreast of changes in the law and its practice*, including the benefits and risks associated with relevant technology* …. [T]he duties of confidentiality and competence … do require a basic understanding of the electronic protections afforded by the technology they use in their practice. If the attorney lacks the necessary competence to assess the *security of the technology*, he or she must seek additional information or consult with someone who possesses the necessary knowledge ….

MODEL RULES OF PROF'L CONDUCT 1.1 cmt. 8.

Lawyers are also required to ensure that anyone working for them conduct themselves in a way that is "compatible with the professional obligations of the lawyer." MODEL RULES OF PROF'L CONDUCT 1.1 cmt. 3. This obligation would apply to the lawyer's employees, agents, and vendors, including document management companies and cloud storage companies. So lawyers are also ethically bound to make sure their companies, such as schools and colleges, managing their client and student files have good cyber hygiene and keep abreast of developments in cybersecurity.

Practical Tips for Effective Cybersecurity Planning

Although cybersecurity plans can vary widely among firms depending upon their business, clientele, and technical architecture, among other things, effective plans include the following features:

Build a Strong Cybersecurity Team

The first step in developing an effective approach to data security is choosing the right information security team. Effective teams are cross-sectional, and include personnel from legal, information technology, human resources, and communications or public relations departments. The team should also include at least one member of senior management.

The New York Department of Financial Services recently promulgated 23 NYCRR Part 500 ("The New York Rule"), a new regulation establishing cybersecurity requirements for financial institutions. Although this rule only affects New York based firms, it provides an excellent model for effective cybersecurity policies. The New York Rule requires financial institutions to designate a "Chief Information Security Officer." The person must be qualified and will be responsible for overseeing and implementing the financial institution's cybersecurity program. 23 NYCRR § 500.04. But the Chief Information Security Officer does not need to be employed by the financial institution. *Id.* A financial institution may instead designate a Chief Information Security Officer who is employed by an affiliate or third party service provider. *Id.* In addition to his or her duty to oversee and implement a cybersecurity program, the Chief Information Officer must also submit a written report to the financial institution's board of directors. *Id.* The report must cover the financial institution's cybersecurity program and material cybersecurity risks. *Id.* While companies outside of New York are not required to follow the New York Rule, appointing a Chief Information Security Officer could be a good place to start for any school looking to build a strong cybersecurity team.

Title search: Cybersecurity Planning

Also available as part of the eCourse
Cybersecurity Planning for Schools: Minimizing the Risk and Mitigating the Impact

First appeared as part of the conference materials for the
33rd Annual School Law Conference session
"Cybersecurity Planning"