CYBERSECURITY 101 – 10 Simple Practice Pointers For Every Lawyer and Client

By Joseph M. Callow, Jr.

Cybersecurity is fast becoming the top concern of Board Rooms, the C-Suite, In-house Counsel and IT Groups in public and private businesses of all sizes. Headlines regarding Target, Anthem, Home Depot, Sony and others have highlighted the breadth and scope of the data protection issue. Whether the threat comes from outside hackers or rogue, disgruntled employees or good people making innocent mistakes, all businesses — including law firms — have to analyze how they are protecting their data and the personal data of employees and customers that they possess.

In this day and age, every business needs to conduct a cybersecurity analysis and have a cybersecurity plan. Different from a document retention policy or a litigation hold policy, a cybersecurity plan is a business-wide plan to protect data and respond to data breaches. Cybersecurity plans are going to vary and should be scalable to the needs of individual businesses — but the underlying common purposes of the plan are twofold: (a) appropriately and reasonably protect data through risk assessment and risk mitigation; and (b) outline an incident response plan to enact when a data breach occurs.

The internet is saturated with articles and sales pieces regarding cybersecurity and it is easy to be overwhelmed with the sheer volume of information on the topic. At its core, cybersecurity is about having a plan and a team of people dedicated to following the plan. To that end, here are some simple pointers and good business practices to help you understand this evolving area of law.

1. Identify Your Data.

Cybersecurity is about protecting data and information — so the first step of any good cybersecurity plan involves understanding where your data is located, how it is being stored (and deleted) and what steps are being taken to secure it.

Data mapping can be challenging. The amount of data created in the normal course of business continues to increase and the sources of data are expanding as well. Data is no longer solely on corporate servers but now may be in cloud storage as well as on laptops, thumb drives, cell phones and perhaps even home/personal computers. Moreover, many businesses also have data stored in legacy systems — the business may not need or use the data, but personal information in old data files may still be valuable to hackers.

Creating an accurate data map for your business is imperative. You need to know what data you have so you can figure out how to protect it (and you should delete data that you no longer need so you can avoid the costs and risk of needless retention).

2. Review Your Policies.

As you understand the sources and location of data, it is important to review your written policies to make sure they match business reality. The policies may have made sense when written several years ago, but they will become outdated as business practices change and evolve. For example, do your policies address data stored on personal/home computers or smart phones/tablets? Do you have a policy covering the use of copying data to thumb drives?

Most businesses now have email, internet and social media policies as well as business equipment, personal device and software access procedures. These policies should define the scope of access to data and set parameters as to what employees can/cannot do with respect to corporate data. Moreover, your policies should have specific procedures that ensure data is retrieved from departing employees and that their access to corporate data is immediately denied.

N.B., HIPAA-related data that qualifies as "Individually Identifiable Health Information" (PHI) or electronic PHI, falls under a separate standard of security and breach notification requirements. Almost all companies possess the protected health information of their employees, and healthcare data is a significant target for hackers. If you have questions about what data qualifies as PHI or ePHI, how to safekeep it and how to address this type of data in your company's incident response plan, speak to someone knowledgeable in this specialized area.

3. Remember Paper.

The focus of most cybersecurity plans is on electronic data and hopefully includes provisions for inactive or inaccessible electronic data as well — but most businesses still have data in paper form in file cabinets or third-party storage sites. According to a January 12, 2015 Report by the Identity Theft Resource Center, over the past five years, 14-26 percent of data breaches involved the theft of data on paper.

Businesses need to make determinations whether to keep data in paper form and, if so, for how long. Businesses also should make sure that document destruction policies are being followed and that documents not subject to litigation holds are being destroyed appropriately.

4. Read NIST's "Preliminary Cybersecurity Framework."

If you are looking for a comprehensive overview of cybersecurity planning, the Preliminary Cybersecurity Framework published by the National Institute of Standards and Technology (NIST) is a good place to start. NIST issued the Framework last year in response to Executive Order 13636, which called for the development of a "prioritized, flexible, repeatable, performance based, and cost effective approach" to managing cybersecurity risk. The NIST Framework provides a step-by-step process for establishing a cybersecurity plan with detailed instructions, charts and diagrams for each step of the process. It is a comprehensive, objective and valuable resource.

5. If the NIST Framework Is Too Techy, Then Read the DOJ Summary.

The NIST Framework is a weighty document. If you want the CliffsNotes version, read the DOJ's "Best Practices for Victim Response and Reporting of Cyber Incidents" Guidance issued on April 29, 2015. The Guidance published by the DOJ's Cybersecurity Unit nicely summarizes the steps to take before a cyber intrusion occurs, the steps to take in responding to an intrusion and advice on "what not to do following a cyber incident."

This Guidance is an excellent summary of best practices and outlines in simple terms what a cybersecurity and incident response plan should contain.

If you need to get buy in within your organization for committing the resources to the development or re-evaluation of a cybersecurity plan, I suggest circulating the Guidance to the various stakeholders and asking, "Are we prepared?"

6. Use Counsel.

When you are evaluating cybersecurity risk and options, involving counsel in the process may help create a privilege that will protect portions of the analysis from third-party discovery. For example, in *Genesco, Inc. v. Visa U.S.A., Inc., et al.*, Case No. 3:13-0202 (M.D. Tenn. Mar. 25, 2015), Defendants sought production of a network security audit performed on Plaintiff's network — but the district court determined that the audit was managed by outside counsel and was therefore privileged.

If you hire a technology consultant to perform a cybersecurity audit or consult on cybersecurity issues, the audit is likely discoverable. If a law firm hires the consultant on your behalf, the audit or consultation may be privileged and protected from discovery in later proceedings. Businesses should consider the benefits of having outside counsel involved in this process.

7. Check Your Insurance Coverage.

Cyber insurance is a relatively new insurance product and the language of coverage and exclusions vary. Some policies have very specific requirements regarding notice, incurment of costs and even which counsel can be used for certain events. Businesses should review their existing policies or comparison shop for cyber insurance policies or riders to their existing coverage.

8. Watch D.C.

Practitioners in this area know

that there is a patchwork framework of rules, regulations and statutes that currently govern cybersecurity issues. Most enforcement is currently done by state attorneys general, although various businesses have industry-specific regulations as well. In addition, 47 states have data breach notification laws, but the laws are not consistent.

Congress and the White House are starting to take the lead in this area. In April, the House passed two bills — the Protecting Cyber Networks Act and the National Cybersecurity Protection Advancement Act — which were designed to create a private-public partnership to share information to help protect against future cyber attacks. The Senate is considering at least five other bills related to privacy and cybersecurity, and the White House has also published its draft Personal Data Notification & Protection Act, which would set national rules on data breach notifications and preempt most state notification laws.

The expectation is that all sides are finally coming together and will enact some form of federal legislation to create a measure of uniformity among the states and likely preempt most existing state laws (possibly near the time of this article's publication).

9. Know Your Third-Party Vendors.

The Target Corporation data breach and several like it are an important reminder that most businesses have to evaluate or reevaluate third-party access to their data. Most businesses allow third-party vendors/contractors to have access to their corporate data; businesses that regularly work in joint venture or joint development relationships likely do as well. Simply having a confidentiality provision in an agreement may not be sufficient protection — and there should be provisions that specifically provide for return or destruction of data when the relationship ends (and checks to make sure that the return or destruction actually occurs). While most businesses focus on their employees, some of that focus needs to be on third-party access as well.

10. Empower a Team.

Cybersecurity is not an IT issue — it is a corporate-wide endeavor that requires input and buy in from multiple players in multiple disciplines (HR, Sales, Risk Management, Operations, C-Suite, etc.). The team should meet regularly, follow trends and have specific roles as part of an incident response plan. Sometimes outside counsel can help provide the impetus for getting the right decision makers in the room, and outside counsel should likely be the first external team member brought into the discussion when an incident occurs.

All businesses need a cybersecurity plan, an incident response plan and a core group of people dedicated to vigorously protecting corporate and customer data. Given the information overload in this area, hopefully these straightforward pointers help you get started with the process.

Callow is a Litigation Partner at the law firm of Keating Muething & Klekamp PLL (KMK Law) and a member of the KMK Cybersecurity & Privacy Team, an inter-disciplinary team of attorneys who advise clients in areas related to protecting corporate data, preventing cyber breaches, and mitigating issues when they arise.