HELPING CLIENTS NAVIGATE CYBER SECURITY LAWS

There is a critical role for lawyers in cyber security planning, and the first step may be to help clients move beyond the hyperbole.

Almost daily we hear news of another spectacular cyber security breach. Examples include the hacking of emails from the Democratic National Committee, preceded by disclosures of confidential information from Home Depot, Target, Wyndham Hotels, Sony, Anthem, e-Bay, and even the US Office of Personnel Management. Worse breaches have occurred involving bank thefts, public safety, medical information and deliberate attacks on US domestic infrastructure. Also disturbing are reports from technical experts that computing technology is advancing so quickly that breaches are impossible to prevent. To increase the level of alarm, most discussions of cyber security begin with an admonition that we should not think in terms of "if we will be compromised," but "when," and the further warning that "it's likely already occurred and we simply don't know it yet."

These warnings are so extreme that a natural response can be to "stick one's head in the sand" and simply avoid thinking about it. Why worry about something that's impossible to prevent? Unfortunately, this view may be particularly acute among small and medium sized businesses who view it as a problem primarily for the super-companies. These small businesses fear that any remedies would exceed their budgets.

The problem with that thinking is that many businesses, large and small, are already within the grip of federal and state statutes imposing duties for handling certain types of electronic information. These are laws "with teeth" and if violated pose substantial risks and liabilities. As lawyers, we are the ones who need to reduce the hyperbole, roll up our sleeves and sort out how to best protect our clients.

I do not denigrate the critical importance of technical specialists involved in this issue. Rather, we simply need to be mindful that the relevant rules and standards of care that will be used in evaluating any sort of liability in this area are legal issues, within the core of what we do as lawyers. In that respect, the highly sophisticated area of computing is not so different from other areas where complex matters are brought inside the law for evaluation and resolution of disputes. For instance we see sophisticated financial controversies, securities and merger transactions, and state-of-the-art scientific disputes involving intellectual property.

Stated differently, there are two components to cyber security. One is the technical, in which computer scientists rule supreme. The other is the determination of the standard of care a particular business must meet and how to manage and mitigate that risk. That's the world in which we lawyers operate, and it's our task to provide guidance to our clients who are attempting to find their way in this new landscape. From this perspective, cyber security needs to be viewed as another 'risk management' issue, which any good business identifies and plans for. Even small and medium size businesses are used to doing that.

The main point of this article is to make the case for approaching the cyber security problem the same way we lawyers address other challenges—methodically, carefully and with a clear view of what the law requires. I also hope it might be an antidote to "sticking one's head in the sand." At the end of the day, if a company does suffer a breach, the remedies and consequences will largely be determined by courts interpreting laws. That's our turf. Even if we don't entirely comprehend the technical issues involved, we do understand what they need to accomplish and by what yardstick they will be measured if a breach occurs. If total cyber security is indeed an illusion, as the tech experts say, then a plan which complies with the law may be the only truly useful goal.

Who Is Covered by Current Federal Laws?

At present, there are sixteen separate federal statutory structures imposing cyber security requirements on businesses. The reach of those federal statutes and rules is very broad. In general, each defines who must comply, the protected information, what constitutes breach, notice requirements, exemptions, remedies, and who can seek enforcement. Unfortunately, those categories may be defined and addressed differently in each statute. Below are just two examples.

The Graham Leach Biley Act (GLBA)

BY KURT HERMANNS

[of Counsel, Gordon Thomas Honeywell]

imposes rigorous cyber security rules on "financial institutions." The definition of that term, however, goes well beyond what we might expect. In addition to banks, it includes savings and loans, credit unions, finance companies, auto dealers, mortgage brokers, utility companies, investment advisors, and other entities involved in extending "credit." A separate but related statute, The Fair and Accurate Credit Transactions Act (FACTA), focuses more particularly on personal identification information and adds telecommunication companies. Between the two statutes and a device called the "Red Flags Rule," an extraordinary number of US companies are required to create a cyber security program, assess risks, provide notices of breach, conduct training, and oversee the program from the operational level up to the CEO and Board of Directors. The statutes direct enforcement by the Federal Trade Commission or the State Attorney Generals, along with penalties and attorneys' fees.

The primary cyber security requirements relating to health care entities are set forth in the Health Care Insurance Portability Act (HIPPA) and the Health Information for Economic and Clinical Health Act (HITECH). These statutes require broad and multilayered protection of personal health information, breach notification to consumers and other formalized cyber security protections. Notably, they apply to health care plans and "business associates," which includes all vendors handling personal health records. The inclusion of business associates makes HIPPA and HITECH extremely broad statutes, reaching from doctors and nurses to any entity involved in the insurance and billing process. They also include complicated regulations concerning how information is adequately protected, breach notifications, and a range of civil and criminal penalties. Enforcement is by the FTC, the US Department of Health and Human Services (HHS), the US Department of Justice, or by State Attorneys General.

There is a patchwork of fourteen additional federal statutory schemes creating special cyber security standards for educational institutions, federally supported housing, telecommunications companies, retirement plans, cable providers, drug and alcohol treatment programs, and homeless assistance programs. Furthermore, any federal government contractor is now subject to detailed cyber security requirements pursuant to the Federal Acquisition Regulations (FARs) and Defense Acquisition Regulations (DARs).

Many of these federal statutory structures limit who can seek enforcement—for instance a federal agency, State AG, or individuals. Nevertheless, courts are already using them to set the standards of care in private causes of action under common law theories of negligence, implied contract, unjust enrichment, and breach of fiduciary duty. In other words, they are being applied beyond the stated limits of the statutes themselves.

What are the State Laws?

Currently, there are 47 states, along with Washington DC, the Virgin Islands, Puerto Rico, and Guam, that have enacted cyber security statutes. As with the Federal laws, they take varying approaches to the definitions of protected information, covered businesses, breach notification, enforcement and penalties.

Washington State has a cyber security statute and strengthened it in 2015. It prohibits unauthorized access of any "unsecured" personal information of a Washington resident held by any business or entity. Encrypted data, using accepted protocols, is not unsecured unless the person gaining unauthorized access also had access to the encryption key or some other means of deciphering the information. The statute further acknowledges preemption if businesses are already compliant with HIPPA, GLBA, HITECH or several other designated federal rules imposing cyber security on banks, credit unions, and other members of the Federal Reserve system. It also waives liability for credit and debit card handling entities if the information was encrypted and such procedures were certified under the security standards adopted by the payment card industry. The Washington statute requires notification to consumers as soon as possible, but not more than 45 days after discovery of a breach, unless it's not reasonably likely to subject consumers to a risk of harm. This notice may be delayed by a request from law enforcement to conduct an investigation. If more than 500 Washington residents are affected the entity must notify the State Attorney General along with a written description and explanation of the breach. Those letters are posted on the AG website—called the "list of shame"—and are available for online public review. Enforcement can occur through either private cause of action or via the AG. If the AG elects to proceed, it may use the remedies set forth in the Washington State Consumer Protection Act.

So What is a Lawyer to Do?

For a business to analyze cyber security as a risk management matter it needs first to identify what statutes apply to its type of business and its types of data. That would require consideration of the full spectrum of statutes. Many businesses will be subject to their own state statute and likely some combination of federal statutes. If it does business in multiple states, those state statutes must also be examined.

The good news is that despite the differences in many of these statutes there are many similarities. In an effort to synthesize these divergent approaches, in 2013 President Obama issued Executive Order 13636. The Order directed the National Institute of Standards and Technology (NIST) to work with government agencies and private businesses to produce "consensus standards" and "best practices" to build a cyber security framework. In essence, those protocols create a template a business can follow in mapping its data, identifying vulnerabilities, planning

for patches, monitoring, planning for possible breaches, and integrating cyber security into the core management of the business. Complying with those protocols, and complying with the applicable statutes, is the path to meeting the standard of care.

In the cyber security litigations thus far, a threshold question for the courts has been determining that standard of care. By and large, the central question posed by the courts considering that issue has been whether the subject business entity had a NIST compliant plan. Stated differently, if the subject business did not have a NIST compliant plan, it likely found itself defenseless in the litigation. Having no NIST plan implies a lack of knowledge of the central issues relating to cyber security, inadequate understanding of special statutory requirements, lack of plans for breaches and protecting customers and, unfortunately, a very large exposure to liability.

A Call to Action

As lawyers, one of our primary jobs is to clarify, plan for, and mitigate risks for our clients. With respect to cyber security, that may mean firmly grasping a client's heels and pulling him or her out of the sand.

The first and most important step is to create a NIST compliant plan. That requires three steps. First, a thorough understanding of the combination of state and federal laws currently applicable to the individual client. Second, a full and frank understanding of the client's current system and its vulnerabilities. This would be best accomplished through a technical investigation conducted within the attorney client and work product privilege. Third, creation of a NIST compliant plan setting forth best practices, monitoring and protocols in the event of a breach.

It's critical that clients understand there is no "one size fits all" approach to this issue. NIST was designed to accommodate a broad spectrum of differences in complexity of systems, types of data and size of budgets. From a legal perspective, it acts as a formalized effort to satisfy the standard of care. If a breach occurs, liability will be determined by the adequacy of that effort and the individual circumstances of the particular client. Without such a plan, the client is unprepared and unarmed.

Kurt Hermanns is 'of Counsel' at Gordon Thomas Honeywell, after a lengthy career with the United States Attorney's Office. He specializes primarily in federal criminal related risk management issues for South Sound businesses.