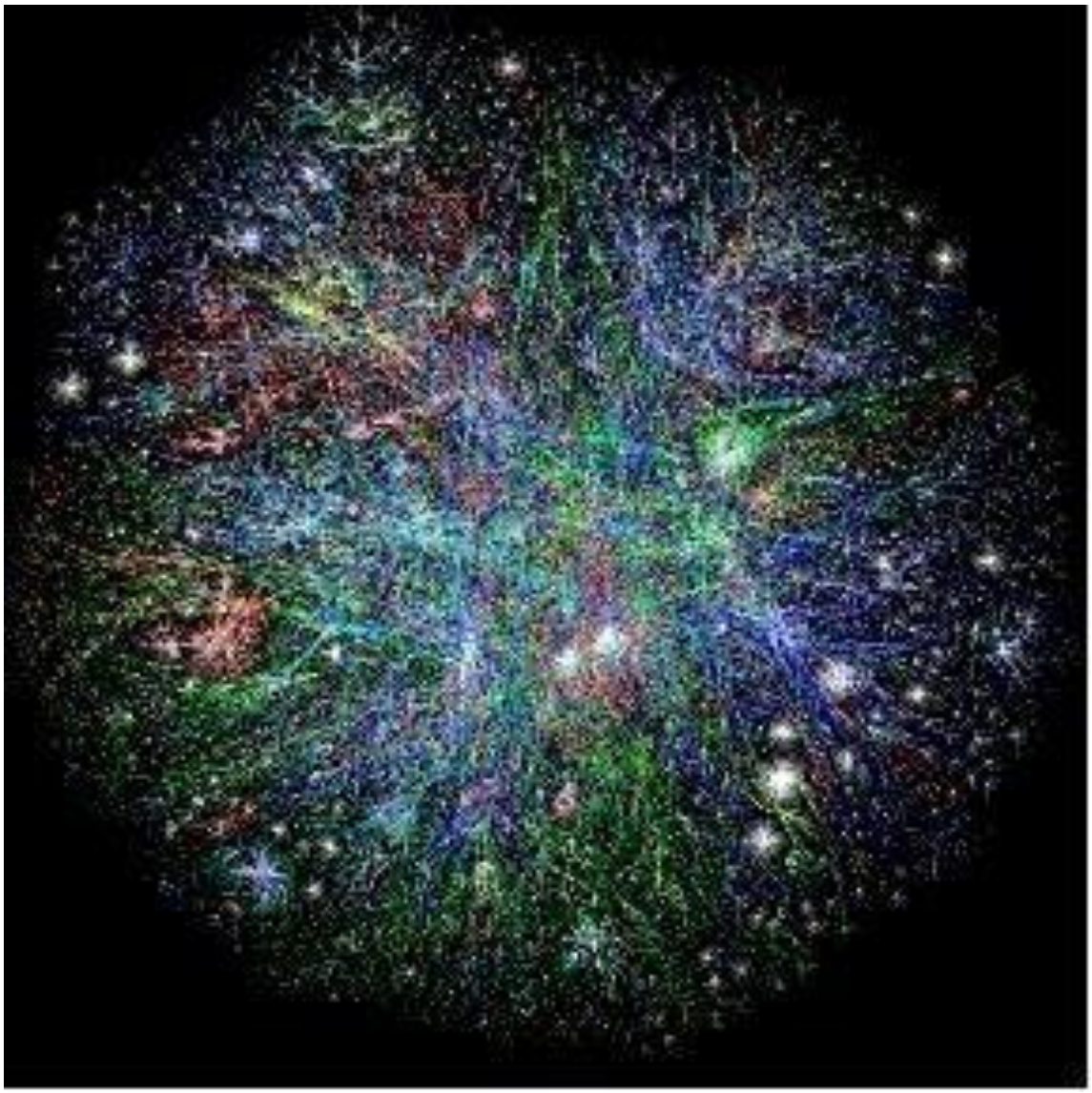
SEIGER GFELLER LAURIE LLP
ATTORNEYS AT LAW

CYBERSECURITY AND THE BOARD OF DIRECTORS

VINCENT J. VITKOWSKY



New York Connecticut New Jersey

SEIGER GFELLER LAURIE LLP
ATTORNEYS AT LAW

CYBERSECURITY AND THE BOARD OF DIRECTORS

Vincent J. Vitkowsky

Cybersecurity is a central concern for insurance company Officers and Directors. One of the challenges they face is that much of the regulatory activity has been *post hoc* and patchwork. The general principle applied is one of "reasonableness." Given the breakneck pace of developments in the cyber domain, this is an especially indeterminate and constantly evolving standard. And there is no clarity as to what measures will come to be viewed as Best Practices. This article provides an overview of the relevant sources of regulation and guidance, and a list of action items and other items for consideration.

Sources of Regulation and Guidance

National Association of Insurance Commissioners ("NAIC")

In November 2014, the NAIC created a Cybersecurity Task Force. In April 2015, the Task Force adopted the *Principles for Effective Cybersecurity: Insurance Regulatory Guidance.* These consisted of a brief discussion of 12 general principles, in essence identifying categories of concerns that regulators should expect insurers to address.

In December 2015, the NAIC Executive Committee adopted the *Roadmap for Cybersecurity Consumer Protections* (previously referred to as the *Cybersecurity Bill of Rights*). It was controversial because it called on insurers to undertake some actions not required under state law. Also in 2015, the NAIC Financial Examiner's Handbook was updated to include market examination protocols for IT security. .

In 2015, the NAIC's Property and Casualty Insurance Committee created an Annual Statement Supplement for Cybersecurity, called the *Cybersecurity and Identity Theft Coverage Supplement.* It requires all companies that provide cyber insurance, either as an add-on to commercial multi-peril packages or as a standalone product, report the range of limits, losses paid, earned premium, whether policies were claims made, and whether tail coverage is offered. On June 30, 2016, it announced the first analysis of the 2015 filings, reporting that that more than 500 insurers have provided businesses and individuals with cyber insurance. The vast majority of the cyber insurance coverage was written as endorsements to commercial and personal policies.

In March 2016, the Cybersecurity Task Force released a preliminary working Draft of an Insurance Data Security Model Law. On August 17, a revised draft was released. Here are some of the key provisions.

- Companies are required to have a written information security program appropriate to the size, complexity and nature of their operations, and are required to document their compliance on an ongoing basis. The Model Act does not indicate what documentation would be adequate, or specify how often "ongoing" is.
- The Model Law states that it does not supersede, alter, or affect any state statute, regulation, order or interpretation, except to the extent that it is inconsistent with the Model Act and only to the extent of the inconsistency. A state statute, regulation, order, or interpretation is not inconsistent if it affords greater protection than the Model Act. There will certainly be issues concerning the exact interaction of overlapping requirements.
- The first draft provided that the obligation to give notice to consumers was conditioned on a "harm trigger." The current draft does not have that trigger.
- In another change from the initial draft, the Model Act does not create or imply a private cause of action, nor curtail any private cause of action that otherwise exists.
- There is a safe harbor for encrypted personal information, and a definition of encryption.
- Although companies are not required to have indemnification from their third-party providers, they are responsible for any failure of those providers.
- Although the initial draft required compliance with the NIST Framework for security programs (see below), the current draft only requires the use of "generally accepted cybersecurity principles."
- It expressly requires oversight of cybersecurity by the Board of Directors.

By insurance industry standards, the NAIC has been moving at breathtaking speed. It is attempting to have the Model Law completed and approved by the end of this year

The New York Department of Financial Services ("NYDFS")

In February 2015, the NYDFS released its *Report on Cybersecurity in the Insurance Sector,* which summarized the results of a survey it had conducted earlier. It indicated the NYDFS would undertake targeted assessments of cybersecurity preparedness; implement new regulations on cybersecurity standards; and increase scrutiny of agreements with third party vendors. It recommended participation in the Financial Services – Information Sharing and Analysis Center. It also made requests to NY insurers for comprehensive risk assessments of their cybersecurity.

On September 13, 2016, the NYDFS announced a proposed regulation, called *Cybersecurity Requirements for Financial Services Companies.* Its major components require companies to:

- establish a cybersecurity program;
- adopt a written cybersecurity policy;
- designate a Chief Information Security Officer responsible for the program and policy;
- have policies and procedures to secure information systems and nonpublic information accessible to or held by third-parties;
- utilize various specific cybersecurity measures; and
- submit an annual certification of compliance by the Board or a Senior Officer.

There is a 45-day notice and public comment period before final issuance.

State Pre-Breach Security Measure Laws Not Specific to Insurers

Some states have general laws requiring pre-breach security measures, generally requiring that they be "reasonable." The California Attorney General has taken it to a greater level of specificity. Its February 2016 Data Breach Report states that failure to implement the Critical Security Controls of the Center for Internet Security constitutes a lack of reasonable security.

Department of Homeland Security ("DHS")

DHS has identified property and casualty insurers as part of the Financial Services Critical Sector. Each year DHS and the Treasury Department produce a Financial Services Sector-Specific Plan. Although their overwhelming focus is on banking, the plans identify risk transfer products, including insurance, as critical services.

National Institute of Standards and Technology ("NIST") Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity

This is a voluntary risk-based compilation of guidelines intended for critical infrastructure industries. It compiles various core practices within the context of five functions. They are: Identify, Protect, Detect, Respond and Recover. These are broken down further into subcategories which describe "informative references" to particular activities, which are meant to illustrate methods to achieve related outcomes.

Federal Trade Commission ("FTC")

The FTC has become the lead agency on enforcement. It has commenced over 60 enforcement actions. On August 31, 2016, it released a paper on *The NIST Cybersecurity Framework and the FTC*. The paper ostensibly was released to answer the question, "If I comply with the NIST Cybersecurity Framework, am I complying with what the FTC requires?" After some discussion, the paper concludes that this is the wrong question. It said: "The Framework is not, and isn't intended to be, a standard or checklist. It doesn't include specific requirement elements. In this respect, there's really no such thing as 'complying with the Framework.' The Framework is about risk assessment and mitigation." The paper then goes on to describe instances in which FTC has brought enforcement actions against companies that did not implement practices that "align" with some of the activities identified by NIST.

Securities and Exchange Commission ("SEC")

The SEC issued a guidance on cybersecurity disclosures in 2011. In essence, it directed attention to the potential materiality of cyber risks, and called for a description a company's relevant insurance coverage. Since then, it has issued several regulations, Market Access Rules, and Compliance Rules in industries other than insurance. In the last year or so, it has brought a targeted series of enforcement actions against investment advisers.

International Association of Insurance Supervisors ("IAIS")

The IAIS released its first paper on cybersecurity in August 2016. It is a general overview entitled *Issues Paper on Cyber Risk to the Insurance Sector*. It identifies some cyber risks faced by insurers, describes some actual cyber incidents involving insurers, and broadly describes the regulatory responses in some European countries, Singapore, and the US. The paper provides a broad introduction to the issues and some of the responses.

(cont'd next page)

EU-US Privacy Shield

The European Union ("EU") regulates the transfer of personal data of EU residents to the US, even within the same organization. Since 2000, that transfer has been enabled by a process known as the Safe Harbor. In October 2015, the EU Court of Justice declared the Safe Harbor invalid on the grounds that it did not provide sufficient protections to EU residents. The decision was largely motivated by the concern that the US Government could access the data once it was in the US.

The EU and US have negotiated a replacement process known as the Privacy Shield, which was formally adopted on July 12, 2016. The Shield is designed to effectuate the same protections for personal data, and rights and remedies granted to individuals as exist under EU law. To use the Privacy Shield, US companies must commit to comply with 7 principles, and 16 supplemental principles, and to take measures so that any entities they transfer the data to also comply with the Shield. Companies are allowed to self-certify their compliance with the US Department of Commerce. The FTC will be the principal enforcement agency.

The current data protection regime in the EU will expire in May 2018. It will then be fundamentally transformed by a new General Data Protection Regulation. The Privacy Shield may not be found adequate under that Regulation. It is also possibly that the Privacy Shield's adequacy under the current regime will again be challenged in the EU Court of Justice.

Actions and Considerations by the Board of Directors

Each company needs to have a specifically-tailored cybersecurity program. As a general matter, Boards should implement the following measures:

- approve the comprehensive enterprise Cybersecurity Policies and Procedures, which need to be continually updated;
- oversee compliance with all of the regulatory sources identified above;
- oversee specific security programs, with established metrics and benchmarks; and
- oversee procedures for reviewing the cybersecurity of third parties with which the company interacts.

In addition, Boards should consider the following measures:

- obtaining cyber insurance;
- establishing a Cybersecurity Subcommittee to the Audit Committee, which could include at least one technical expert, to make recommendations to the Board on its cyber responsibilities;
- requiring quarterly cyber reports and updates (the NYDFS Study stated that only 30% of Boards receive updates that frequently);

- pre-approving cybersecurity software, hardware, and consultants;
- retaining, and overseeing any security firm engaged by the company;
- retaining independent security experts to assist the Audit Committee and any Cybersecurity Subcommittee;
- overseeing the identification and pre-breach retention of digital forensics experts and data breach response professionals, including attorneys; and
- consider appointing a Director with cybersecurity expertise.

September 2016

Vince Vitkowsky is a partner at Seiger Gfeller Laurie LLP, resident in New York. He serves insurance and reinsurance companies in litigation, counselling, and product development in many lines of business, including cyber, E&O, D&O and CGL insurance. Vince created a Cybersecurity Podcast and Symposium Series featuring leading cyber experts, consultants, present and former government officials, and journalists. Over the years, he has been included in various directories of leading lawyers, including Chambers America's Leading Lawyers for Business (describing him, among other ways, as "a well-prepared operator") and Euromoney's Best of the Best. He can be reached at vvitkowsky@sgllawgroup.com. More information on Seiger Gfeller Laurie LLP can be found at www.sgllawgroup.com.