Deloitte.

Operational Integrity Enhancement

Insurance Industry Analysis

CENTER *for*
REGULATORY
STRATEGY
AMERICAS

Insurance

Relative to the banking and securities industries, the insurance business is a bit less central to the daily functioning of our capital markets. As such, regulations related to operational integrity in insurance are still emerging—and in many cases, insurance regulators and other standard-setting bodies are following the lead and lessons learned from their counterparts in banking and insurance.

Regulating operational integrity is uniquely challenging in the insurance industry because of its state-based regulatory structure—and by the fact that some of the larger, more diverse insurers are also subject to operational integrity regulations established for other industries in which they are involved. For example, AIG and Prudential are not only subject to oversight from insurance regulators, they must also comply with the requirements imposed on Systemically Important Financial Institutions (SIFIs) as defined by the Dodd-Frank Act. Similarly, insurance businesses that include a depository/banking component are also subject to regulation by the Fed.

Cybersecurity is the main threat to operational integrity in the insurance industry—a threat highlighted by a number of recent cyber intrusions against insurance companies that have been very costly, both in terms of reputations and financial performance. Such attacks also raise concerns about privacy and confidentiality since insurance companies hold vast quantities of sensitive and personal data about their customers.

One of the toughest challenges with cyber threats is their diffuse and varied nature. Some threats come from external sources such as highly sophisticated state actors, cyber activists, or traditional criminal organizations. These external threats are difficult to guard against. However, it can be even more difficult to guard against internal threats such as employees who do not practice proper cybersecurity or rogue contractors that have access to a company's systems. Adding to the challenge is the fact that today's increasingly customer-centric insurers must fully secure their cyberperimeters while, at the same time, make new and existing customers feel welcome.

Here are some key operational integrity trends to watch in the insurance industry:

Cybersecurity Bill of Rights. To help address the cybersecurity threat, the National Association of Insurance Commissioners (NAIC) recently formed an executive task force to raise awareness and increase regulatory oversight. The task force has drafted a Cybersecurity Bill of Rights that is designed to alert consumers about the protections they should expect in the event of a data breach (including rights such as full disclosure and free credit monitoring). However, the document also effectively serves as a guide for both regulators and insurers about the protections that should be offered by the industry. At the moment, the Cybersecurity Bill of Rights is working its way through the feedback and approval process, and widespread adoption at the state level is likely to happen soon. In fact, New York is already proactively moving to incorporate key elements into its insurance regulation and legislation.

FFIEC Cyber Assessment Tool. Regulating something as fast-moving and cutting-edge as cybersecurity can be a real challenge for insurance industry regulators, which by nature tend to be reactive and positioned a step or two behind the entities and business threats they are expected to regulate. As a result, insurance regulators are increasingly

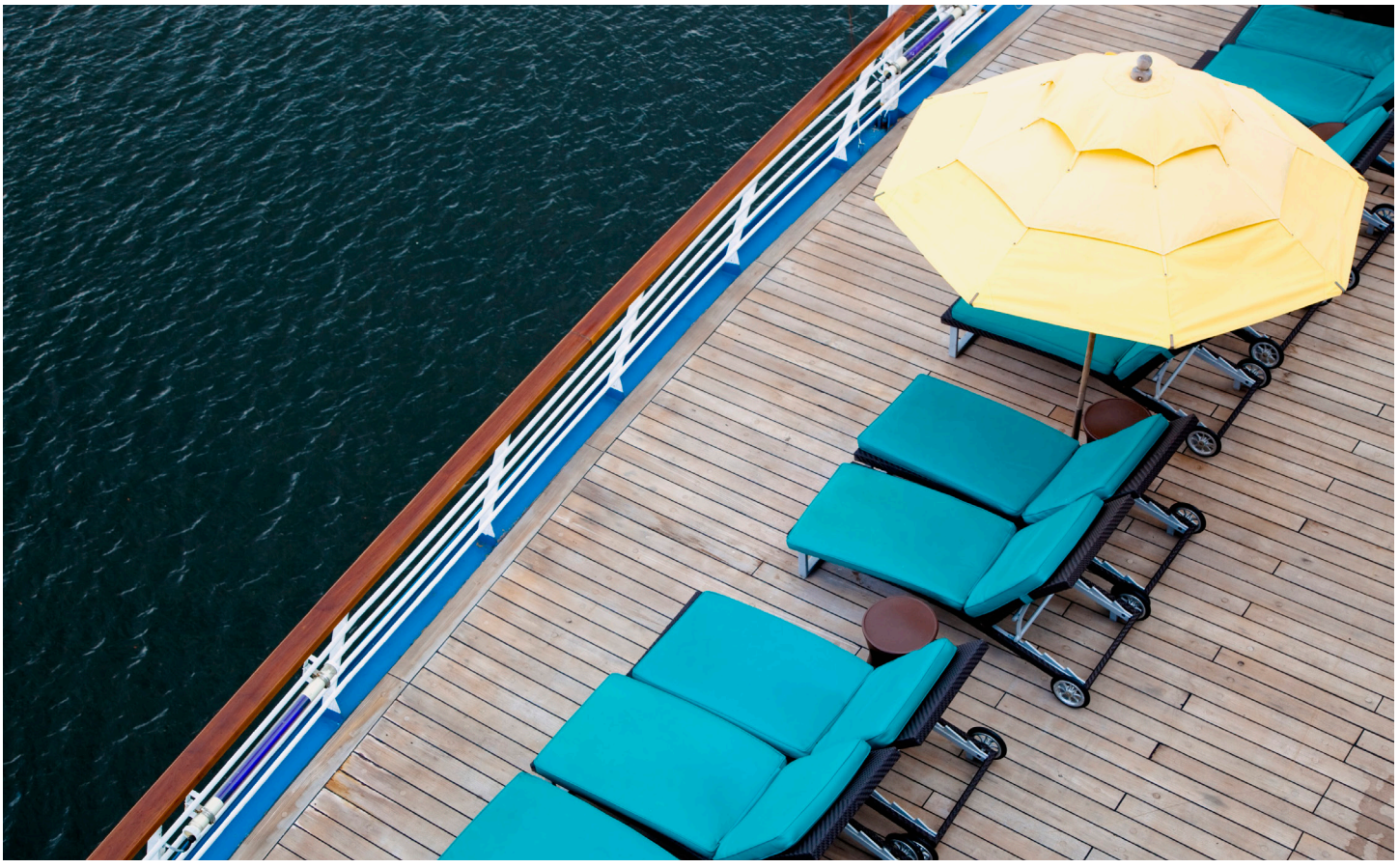
looking to leverage the latest and greatest tools developed in other industries. Using this approach, cybersecurity has now been fully integrated into the insurance industry's regulatory examinations. Specifically, according to the NAIC, everything covered by the FFIEC Cyber Assessment Tool is now included in current insurance examinations.

Principles for effective cybersecurity. Insurers looking for a holistic, principlesbased approach to cybersecurity may want to consider using the NAIC's principles for effective cybersecurity, which are based on NIST's standards. These are constantly being updated to reflect the latest threats and thinking.

Increased focus on models. Sophisticated mathematical models play a key role in many aspects of the insurance industry, from underwriting to investments to storm prediction. As such, regulators are starting to focus more attention on the quality and reliability of the industry's models. This includes not only a clear understanding of what the models do and how they work, but also how accurate they are, who builds them, and what kind of data goes into them (and how that data is stored and managed).

Enterprise risk management. The NAIC's principles include a very basic, but sometimes misunderstood and overlooked concept: that cybersecurity extends beyond the information technology department and must include all facets of an organization and be a part of an enterprise-wide risk management process. Cyber war games, systems, assessments, and periodic employee training are just some of the tools insurers are increasingly using to discover and reduce vulnerabilities. In addition, the NAIC believes it is essential for insurers and producers to use an information sharing and analysis organization to share information and stay informed about emerging threats or vulnerabilities.

Own risk solvency assessment (ORSA). This reporting requirement, which took effect in July 2015, has the potential to lift enterprise risk management to a higher level by providing a truly customized and comprehensive view of risk across the enterprise, covering everything from corporate culture and governance to ownership of risk. However, in its current form, ORSA's only requirement is to file an assessment report; there is no mechanism for measuring and enforcing the quality of the report. This could change soon, however, since regulators are already under significant pressure from ratings agencies and others to make formal value judgments about the quality and completeness of the assessments. As an intermediate step, regulators have started to publish examples of ORSA leading practices.



Contacts

Howard Mills
Managing Director
Deloitte Advisory
Deloitte & Touche LLP
howmils@deloitte.com

CENTER *for*
REGULATORY STRATEGY
AMERICAS

The Deloitte Center for Regulatory Strategy provides valuable insight to help organizations in the financial services, health care, life sciences, and energy industries keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends.

Home to a team of experienced executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the Center exists to bring relevant information and specialized perspectives to our clients through a range of media including thought leadership, research, forums, webcasts, and events.

Deloitte.