INVESTMENT COMPANY INSTITUTE®
ICI Global
WASHINGTON, DC • BRUSSELS • LONDON • WWW.ICI.ORG

ICI VIEWPOINTS

OCTOBER 3, 2017

Cybersecurity at Work: To Confront Evolving Threats, Flexibility Is Key

By Peter Salmon

Part of a series of ICI Viewpoints *covering cybersecurity issues.*

In the previous installment of this series, I examined a few ways to think about the cyberthreats facing us, and thus to guard against them more effectively. Now, with organizations in every sector of the US economy facing increased pressure to safeguard corporate and client data or suffer potentially ruinous damage to their operations and reputation, it seems that some regulators think they should dictate what's best for all of us, regardless of individual firm circumstances.

The mutual fund industry has long taken seriously its obligation to protect the confidentiality and integrity of nonpublic shareholder information against any threat—including cybersecurity threats. Federal and state regulators, for their part, appear to be concerned as well. After all, there is no shortage of cybersecurity regulations and guidelines. But now we're facing a risk of going too far: 48 states currently have their own privacy standards, while any number of federal agencies are regulating content and notice requirements.

The prospect of each of the 50 states issuing cybersecurity standards on top of cyber initiatives promulgated by federal financial-services regulators is daunting. Worse, such a proliferation of standards could create conflict that would end up making it harder for funds to secure shareholder information. And regulators' natural temptation too often is to try to prescribe the one "correct" way to secure systems and data—turning standards into rules. For example, is it truly useful to require that a firm name a chief information security officer? Frankly, the job functions, responsibilities, and skills of an individual are more important than any title.

Coordination and harmonization among regulators is the best path forward—as long as the outcome is a principles-based framework, rather than a patchwork of prescriptive checklists that could quickly be exploited by hackers and other adversaries.

Getting to What Works in the Real World

We already know how such a principles-based framework can work, because the mutual fund industry has been practicing robust cybersecurity under just such an approach.

Through current and past guidance and alerts, the US Securities and Exchange Commission (SEC) has effectively established the appropriate direction for fund managers to follow—while affording the necessary flexibility for each firm to tailor its cybersecurity program to its business structure, technical architecture, investor base, and unique set of threats. ICI members use this flexibility and guidance extensively to create, maintain, and develop their cybersecurity programs.

One example of a tried-and-tested foundation of security controls rolled into a voluntary framework came in 2008, when an international grassroots consortium of companies, government agencies, institutions, and individuals developed what is now known as the Center for Internet Security Controls for Effective Cyber Defense. The controls were designed to:

- help organizations define the starting point of their defenses;
- direct scarce resources in a way that would achieve maximum benefit; and
- focus on the additional risks unique to their business.

The controls also map directly to the core requirements of the National Institute of Standards and Technology (NIST) Framework for

Improving Critical Infrastructure Cybersecurity, which provide a principles-based approach for making certain that a security program is effective and efficient against real-world threats.

ICI members clearly prefer this approach. Data from the Institute's 2017 Cybersecurity Benchmarking Survey show that fund firms responsible for managing the vast majority of the industry's assets model their information security programs against an amalgam of standards and benchmarks. In other words, firms choose to adhere to those parts of different frameworks that make the most sense, given the unique needs and risk profile of their firm. They are able to follow this approach because the industry's primary regulator—the SEC—has given them the flexibility to do so.

Flexibility Works

Simply put, good cyber hygiene is about doing what works—that is, getting the basics right and working effectively in your unique environment. Clear, evidence-based guidance and controls already exist in the form of the frameworks mentioned above, and can provide both federal and state regulators with the assurances they seek.

The SEC gets this. It continues to demonstrate flexibility by using guidance and alerts to inform the mutual fund industry of appropriate cybersecurity responsibilities, which fund sponsors address through such thoughtful approaches as the NIST Framework. What the fund industry and its 95 million shareholders don't need is for other federal and state regulators—which have only a passing familiarity with the industry—to promulgate their own sets of rigid standards that ultimately would distract fund firms from focusing on efficient and effective cybersecurity priorities and practices.

The next post in this series will examine the insider threat.

Additional Resources:

- Information Security Resource Center

Other Posts in This Series:

- Cybersecurity at Work: Creating Passwords That Are More Secure
- Cybersecurity at Work: Incident Response Plans and What They Entail
- Cybersecurity at Work: Exercise Is Important
- Cybersecurity at Work: The Benefits of Information Sharing Networks
- Cybersecurity at Work: The Risks of Information Sharing
- Cybersecurity at Work: Keeping Secure When Away from the Office
- Cybersecurity at Work: I Know What You Know!
- Cybersecurity at Work: To Confront Evolving Threats, Flexibility Is Key

Permalink: https://www.ici.org/viewpoints/view_17_cyber_08

Peter Salmon is ICI's senior director of operations and technology.
