The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE
Washington, DC // Brussels // London // www.ici.org

ICI VIEWPOINTS

APRIL 20, 2016

Cybersecurity at Work: Exercise Is Important

By Peter Salmon

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

In this installment of our series focusing on cybersecurity, we are going to look at exercising—not the type of exercising that many of us do to stay in shape, though that is a good place to start. There are myriad reasons why people exercise, including to get or stay in shape, improve a skill set, strengthen weaknesses, or be better prepared for competition. These reasons also apply to the corporate world, where organizations do their own exercises—fire drills, business continuity plans, active shooter scenarios, etc.—so that employees are better prepared when something bad happens. Cybersecurity preparedness is no different.

In our last post, we wrote about the importance of incident response plans, as well as some important components they should include. Yet a well-thought-out incident response plan that sits on a shelf and does not get exercised or updated is not fulfilling its purpose. These plans need to be tested—exercised—so gaps are identified, changes made, and mitigation strategies improved. Likewise, staff members need to get comfortable with their roles and responsibilities during a serious cyber incident. Like many endeavors, what is required is practice, practice, practice.

One type of practice session is known as a tabletop exercise. Let's look at some aspects of what makes for a good one, drawn from an excellent guide created by the U.S. Department of Homeland Security.

Assuming you've already identified the correct participants, when conducting a cyber tabletop exercise, you want to first set a goal regarding the scope of the scenario you will simulate—for example, a distributed denial-of-service attack—and detail how complicated you want the exercise to be. You also should establish separate goals for what you want the test to accomplish—for example, how well existing policies and procedures are designed to respond to a threat, and whether or not contact information is up to date. As your firm steps through the scenario, the exercise will provide an opportunity to validate this and other information. It is important that someone document the exercise's findings, so any gaps in procedures can be addressed as appropriate.

There are some challenges associated with a tabletop exercise that you should recognize. For example, it will likely come as no surprise that some participants will be less excited than others to take time away from their daily responsibilities to walk through a test exercise. So, to get the most value from the time spent exercising, it's important to take time to plan the scenario well.

Another challenge involves time—or, more precisely, the lack of it. Small firms in particular may find it a bit more challenging to find an acceptable time to conduct the test, especially as test scenarios become more complicated and require employees to take an entire day or more to work through an exercise. Organizations need to keep in mind, however, that the benefits of a good test in identifying vulnerabilities will prove extremely valuable during a real event.

A component of these exercises usually includes a penetration test, either announced or not. Such tests—which attempt to gain access to information systems without knowledge of usernames, passwords, or other normal means of access—can enable an organization to measure many aspects of its information security program, including:

- the time it takes to detect and respond to abnormal network activity;
- the time it takes to declare an incident;
- whether incident-response procedures are followed; and

- the effectiveness of personnel and equipment.

It is during a test that you want to “fail”—or, if you prefer, to find any existing gaps in processes, procedures, or equipment that can be remediated, enabling the firm to be better positioned to counter a real attack. For some smaller firms, this may seem overwhelming, but remember: tabletop exercises can be as simple or as complex as appropriate for the firm.

Just as when you exercise your body, it may be difficult at first, but with regular practice, you’ll get used to it—and better at it. Organizations that have a plan and test it regularly through tabletop and other exercises will find that they perform better under more difficult conditions. Weightlifters like to say, “no pain, no gain.” In this case, the long-term gain will be more than worth the initial pain.

Join us next month, when our next post will answer this question: what is an exchange of data between organizations, people, and technologies?

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

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