The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

ICI VIEWPOINTS

March 21, 2016

Cybersecurity at Work: Incident Response Plans and What They Entail

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

In this second posting in our series, I'd like to focus on computer incident response planning. In last month's post, I mentioned that there are many more data breaches that take place than we are made aware of through the media. These cybersecurity events can affect networks large and small, from large multinational corporations to your own home.

It is natural to have emergency plans in the event that something bad happens—ships have life rafts, planes have oxygen masks, and I have a backup battery for my tablet. However, not every computer security incident rises to the level of enacting a full-blown incident response plan. There are many elements to consider when creating and implementing a robust incident response plan—some of which are covered very well here—but let me highlight a few, beginning with defining what constitutes an incident.

The Importance of Planning

Defining what constitutes a computer security incident is not as simple as it may first appear. In fact, the choices are almost limitless. For example, my computer shutting down is an "incident," but not one that requires me to notify my computer incident response team (CIRT). On the other hand, internal and external network breaches, unauthorized network access, malware infection, and distributed denial-of-service attacks are some examples of incidents that *do* require the attention of a CIRT. The scope of incidents that a CIRT will respond to should form the basis of your incident response policy. Of course, your firm's organizational structure, as well as roles and responsibilities laid out in the organization, will also help inform this policy.

Though we cannot possibly cover all aspects of computer incident response plans in this post, we can emphasize the need to prepare and plan. When is the best time to figure out if your firm has identified the correct staff to be part of the CIRT? To figure out whether they have the appropriate skill set? To figure out whether you have senior management support, etc.? Hint: it's *not* the moment you discover a data breach. A collaborative and proactive approach will facilitate quick communications and response. Building out an incident response policy and creating a plan based on it will help you identify your short- and long-term goals, as well as identify ways to measure the plan's effectiveness going forward.

Document, Test, Enforce

As you work through your plan, policy, objectives, and the like, it's important that they be written down. It's also crucial that you follow your plan and procedures if an event occurs.

In other words, do what you say you are going to do. Experience is great—but it isn't a plan. It's wonderful to have an experienced individual on your CIRT, but relying primarily on someone's "institutional knowledge" during an incident is not much help if the person is unavailable or if you are facing a new threat.

On a related note, make certain you have a well-thought-out and documented escalation procedure. Keep in mind that regulators and auditors not only will want to see evidence of a plan, but they will want evidence that it has been exercised. Running tabletop exercises to assess the practicality of a plan—enabling you to make adjustments, assign accountabilities, and identify items missed—is critical. A plan without practice may give a false sense of preparedness, and could lead to an unpleasant outcome.

One final thought on computer incident response plans: they should include a law enforcement component. Before a breach or some other cyber incident occurs, contact your local FBI and U.S. Secret Service field office and get to know the agents in their respective cybercrime units. The time to understand law enforcement's investigative capabilities and expectations is *now*—not during a breach. It's a good idea to involve your general counsel in these discussions, so he or she is not surprised by the nature of requests from law enforcement during a breach. In addition, once you have a relationship with the appropriate federal law enforcement agents, maintain that bond as you would any other important relationship.

Our next post in this monthly series will ask, what is a an eight-letter word that means performing or practicing to develop, improve, or display a specific skill?

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

---