TABLETOP WAR GAMES

This week I participated in a simulated cybersecurity incident exercise—a tabletop War Game—with Austin's chapter of the Information Systems Security Association. Participants in the War Game each represented parts of a business responding to a cyber incident, including the C-suite, Legal, Engineering, Public Relations, and Customer Service (I played the General Counsel). We were given the facts of the incident real-time as they "happened" and we responded real-time with recommended actions and advice. The audience played the role of the general public, peppering us with customer complaints and investor questions to complicate our deliberations and actions.

This rapid-fire event was a great test of the panel's problem-solving skills, ability to work effectively with others under pressure, and expertise. And it highlighted for me some simple takeaways applicable to any person—whether legal, technical, or otherwise—who may play a part in a cybersecurity incident.

1. **Have a plan.** Going through a cyber incident is living in a pressure cooker—the heat is on and everyone is testy. In the heat of an incident, you need to devote brain power to stopping the attack, preventing damage, and recovering your business. You shouldn't spend precious time defining roles and responsibilities, navigating political issues in your business, or deciding whose budget should cover the experts you engage. In our simulated event, the participants worked very well together due in part to their positive personalities, but also to the fact that we were provided a written plan as part of our scenario. Without the written plan, I bet we would have debated many more issues than we did, which wastes time you don't have during a live incident. Having a defined plan created outside the heat of the moment and that addresses as many "what ifs" as possible allows a team to work better together in crisis, leading to a better overall result.

2. **Know your plan and policies.** Although many companies have written incident response plans, I think once completed there is a tendency to put the plan on a shelf and rarely revisit. It is critical not only to test your plan and update it regularly, but for the personnel who will be called into action by the plan to be familiar with the plan. Creating an operational response plan, checklists, phone trees, or other quick reference guides can also ensure your plan is easy to understand and execute during an emergency.

3. **Know your business.** One issue that came into sharp focus for me during this simulation was the value of knowing your business. Many people, especially at larger companies, are hyper-focused on their area of expertise and lose sight of, or just aren't familiar with, the big picture of the business. In our simulation, the participants only learned about our company and product lines at the beginning of the exercise, so we spent a lot of time agreeing on actions, only to have to backtrack because we hadn't considered the impact to all of the product lines and different customer types. Your customer base—whether consumers, businesses, or government—and products impacts the way you respond to an incident. You should familiarize yourself with all of these things in advance of an incident. It is also important to have a high-level understanding of your IT infrastructure. In a critical situation where time is of the essence, people are prone to clutch the life raft without inspecting it for holes, adopting a remedial measure that quickly solves one problem without realizing the unintended consequences that could harm your business. Knowing your business ahead of time will help you spot these issues and land more quickly on a solution that won't cause additional harm.

While having a written plan is the first step to being ready for a cyber incident, these additional practical considerations are also important to cyber incident readiness. The War Game simulation was a fantastic exercise to validate our beliefs about cyber readiness and to see them play out live.

Sincerely,

The Insider (aka: Renee Meisel)