Texas Council Risk Management Fund

Incident Response Plan Testing

As part of the TCRMF Cyber Risk Control Program, an IT Risk Control Assessment is used to identify gaps in controls and processes. It is an important "self-scouting" procedure in which all IT environments should partake. After producing several assessment reports for members, an area of improvement that is commonly noted is the inability to test plans such as an Incident Response Plan. We find plans that are in place but have not been tested.

Incident response plan testing is used to determine whether an incident response process is effective and identifies critical gaps. Testing helps to ensure all members of the team are aware of and familiar with their roles and responsibilities. Any gaps could cause issues if a real attack occurred. It is important to detect any vague or ineffective areas of the plan before the plan is ever used. We will discuss the Tabletop method for testing Incident Response Plans.

Tabletop Exercise
This is the most basic test of your incident response plan. All the key members of your Incident Team meet in a conference room and go over several breach scenarios. Members are asked to talk through their part of the response, as directed by the plan.

There is definite value from this approach. In most organizations, questions like the ones below, used in a Ransomware scenario, tend to highlight some holes, and generate some meaningful to-do items after the meeting.

How do you investigate and discover what was exfiltrated?
How long will it take to recover data from backup(s)?
What are the talking points for staff who get calls from customers?
How will the multiple DDoS attacks be mitigated?
What vendor agreements are in effect?

A broad range of scenarios such as Ransomware, Business Email Compromise, and Cyber Extortion are encouraged to be examined when testing.

Incident response capabilities need to be put to the test. It is important for ALL employees to understand their role in the cyber security of the organization. Responding to cyber incidents and breaches is an organization-wide effort, which is why clearly defining who needs to do what in your response plan is critical before you even begin to test it.

The TCRMF Cyber Risk Services Advisor, Lee Cain, has started to schedule Incident Response Plan Tabletop Testing visits for members. To get on the schedule, email Lee at Lee.Cain@sedgwick.com, or call him at 512-619-1437.