CampusGuard News 3/1/2020

Incident Response: Key Players in a Tabletop Exercise

Requirement 12.10.2 of the PCI DSS requires organizations to review and test their incident response plan at least annually. The DSS isn't specific as to how this should be performed, but gathering everyone in one room for a discussion-based tabletop exercise can be a good way to test your plan and verify that all appropriate staff members understand their individual roles and responsibilities.

Whether you are focusing specifically on PCI and a potential breach or compromise of cardholder data, or a more general cybersecurity incident, a tabletop exercise should not require extensive resources and allows you to test a potential real-life scenario in an informal environment without any real risk to your organization. Your team will gain the experience of walking through the test together, coordinating efforts, identifying gaps or weaknesses in the overall processes, and making changes to your incident response plan as needed. It is much better to identify snags during a test, than it is to try and figure out next steps during an actual incident.

Along with planning for an appropriate facility and selecting a date, you will need to determine who from your organization needs to be involved. All relevant parties should be engaged in the planning process as appropriate so you can ensure their participation and buy-in. You want key decision-makers in the room, as well as operations personnel that can bring experience and new ideas to the table.

Organizations must assess what staff members will benefit most from the exercise and what potential roles they would play if a real event were to occur. You will want to include anyone that could be impacted or might play a role during the incident scenarios. Some questions to ask when you are building out your invite list:

- When a suspected incident occurs, who is notified first? (Help desk, IT Support, etc.?)
- Who should be contacted immediately?
- Who is responsible for handling the situation?
- Who would need to know if an incident had occurred? (Executives, HR, Legal, Communications)
- What if those individuals are not available or are out of the office, who is their backup?
- Who will handle communications if this incident needed to be shared publicly?
- If outside agencies are involved, who would manage that?

Below are some of the different roles to consider when you are planning a cybersecurity-focused tabletop exercise:

- Managers
- Front-line employees
- Help desk staff

- Information Technology - local and central (if applicable)
- Information Security
- Cash Management/Treasury (if payment card/financial related)
- Senior leadership – VP, CFO, CIO, CISO, Controller
- Communications/Public Relations staff
- Campus Police/Local Police
- Public Safety
- Maintenance
- Internal Audit
- Legal

The tabletop exercise should help strengthen relationships between the different groups and team members that may not interact in their daily roles. This can be a great way to break down silos and jumpstart constructive conversations across the organization. It can also help everyone gain familiarity with other stakeholders, and make it much easier for team members to reach out to people they have worked with in the past during an actual incident. Knowing who and when to contact each group or individual is important. Once you have narrowed down who is most relevant, you can work to define their roles during the practice scenario. During the test, you can also verify all contact information is up to date and confirm that you have an escalation call list in the event something happens when critical personnel are out of the office.

Having a well-thought out tabletop exercise and ensuring the right people are in the room will make a big difference in the success of your trial. For other questions about how to plan a tabletop exercise, don't hesitate to reach out to your dedicated CRM Team.

Additional guidance from our Security Advisor team below:

[Hobby]: *Tabletop exercises are an excellent way help organizations consider the risks of cybersecurity threats and provide an opportunity to raise awareness and improve understanding of how to respond to those threats and other issues. Participants deal with real-world cybersecurity events designed to promote information sharing among the represented departments and organizations. Participants talk through issues, discuss how they believe their organization would handle situations, and identify related best practices and areas for improvement.*

Having all the key players at the table is important because participation and interaction are used to build cohesiveness among the participating organizations. The exercise allows the participants to share their experience with colleagues and counterparts. Participants gain insights from each other's perspectives and their discussions increase their cybersecurity awareness as well as their familiarity with the incident response process. When it comes to the participation of key roles in tabletop exercises, more really is more.