fortium partners

Case Study

Preparing Financial Leaders for Deepfake Cyber Attacks: A Case Study

Client Profile

- Industry: Financial Services
- Annual Revenue: $5B
- Employees: 2,500
- HQ: Washington state

The Challenge

Before Fortium's engagement, a prominent financial services company knew that it was not prepared for cyber attacks involving deepfake artifacts and synthetic identities. Since the company had a previous incident that demonstrated its lack of preparedness, it engaged Fortium Partners to develop a tabletop exercise tailored to its operations. The process would be designed to stress test the Board of Directors' and executive management's ability to effectively handle such an attack and provide recommendations for closing any gaps.

Key challenges:

- **Understand the company’s business:** In order to develop a plausible scenario for the tabletop exercise, Fortium Partners needed to thoroughly understand the client’s business, operations, and security posture as well as the regulatory environment in which it operates.
- **Leverage the Board and Executive Management Structure:** In advance of the exercise, the following questions needed to be addressed:
  - Who will be participating in the tabletop exercise?
  - What are their responsibilities? What are their areas of experience and expertise?
  - What are the roles and responsibilities of the Crisis Management team members (including the board)?
- **Identify the company’s risk appetite:** Just how realistic should the deepfake exercise be? Fortium Partners needed to sufficiently stress test the client’s incident response planning without triggering unintended consequences from the client’s response to the scenario.
- **Develop infrastructure and artifacts:** Fortium Partners needed to build the infrastructure and develop the exercise artifacts necessary to support the synthetic identities and deepfake artifacts required to simulate a real world scenario.

- **Financial Services Compliance Requirements:** Given the breadth of industry expertise, Fortium leveraged their Partners' thorough understanding of the financial services regulatory requirements in order to bring as much realism as possible to the exercise scenario.

The Solutions

To address the critical challenges and mitigate risks, Fortium Partners implemented the following:

- **Assembled a cross-functional team:** Fortium utilized a cross-functional team comprising both CISO and CIO partners with in-depth industry knowledge for the engagement.
- **Worked with a trusted insider:** Fortium worked with a trusted insider, a senior client employee, who was integral to the scenario development to ensure that Fortium was meeting the client´s objectives. This was critical since this was a targeted exercise for the Board of Directors and executive staff. During the actual tabletop exercise, that trusted insider was restricted to only observing.
- **Built a comprehensive infrastructure to support the scenario:** The infrastructure and artifacts developed to support the scenario were customized specifically for this client to ensure maximum benefit. At the conclusion of the exercise, the infrastructure was dismantled, and the artifacts were given to the client, not to be used with any other Fortium client, in order to preserve the client's confidentiality.
- **Facilitated exercise:** Two Fortium partners were on-site to conduct the exercise, facilitate it, and capture information for the after-action report: lessons learned to be delivered to the client.
- **Adapted the scenario to real-time events:** The two onsite Fortium partners were able to adapt the scenario in real-time based on discussions and actions taken by the exercise participants.

The Results

Fortium Partners' engagement resulted in a highly successful tabletop exercise. This initiative enabled the client to test its incident response plan and update it to address a new type of attack involving synthetic identities and deepfake artifacts. The client's feedback was overwhelmingly favorable in its ability to elevate the readiness and responsiveness needed to mitigate and manage any future deepfake attacks.