CASE STUDY

Incident Preparedness: A Prescription for Cyber Resilience.

The complexity of today's cyber threat landscape requires organizations to not only protect their cyber security controls, but to also be sufficiently prepared to handle a security breach. In the case of healthcare providers, an increasingly acute concern is an ineffective incident response coupled with the potential loss of sensitive data, quality of service, and patient trust.

Trustwave®

Client Spotlight

A major metropolitan health services provider was seeking guidance on the efficacy of its existing incident response processes. The provider had comprehensive plans but was concerned about a ransomware attack involving another provider in the same region. The adjacent attack resulted in healthcare service delivery interruptions impacting patient care for hospitals in the area.

The Challenge

Since no two security incidents are the same, an effective response is not simply about having documented plans and playbooks in place, but it is also about testing the response to the latest style of ransomware attacks with the most up-to-date processes, tools, and people. Defending a system requires multiple levels of operational staff, senior management, multiple departments of HR, Legal, PR, and IT - all working in concert to efficiently execute the latest response plans under pressure.

Industry Threat

Healthcare organizations, especially hospitals, have always been a particularly susceptible target for cyber-attacks given the sensitive commercial and patient data they hold, as well as the patient care implications of system downtime. Moreover, they have come under vastly increased operational pressure due to the COVID-19 pandemic. In this context, the effects of a successful cyber-attack can have catastrophic consequences if not handled expediently and with expertise.

The Solution

Trustwave used its significant experience in breach response to design a custom Tabletop Exercise with the client's crisis management team. The exercise simulated a sophisticated ransomware attack that resulted in the compromise and encryption of key systems storing patient data. Throughout the half-day session, the Trustwave consultants presented the ransomware scenario along with a series of variables from the possibility of insider involvement to the leakage of patient data and the need to handle media inquiries as the mock incident becomes public.

A large component of the exercise is to simulate the sense of pressure and uncertainty of a real incident. The crisis management team was prompted at various points during the response to answer questions that would demonstrate their thinking processes and how they might work together to contain the incident using the documented incident response processes, while managing the operational impacts of the incident.

As a result of the Tabletop Exercise, the client gained important insights on the effectiveness of its incident response capabilities and the potential areas for improvement. It also gave the team firsthand knowledge of how well the team might work together under pressure as well as providing an opportunity for them to understand the interplay between the containment of the incident from both an IT and business operations perspective with broader business considerations including operational and stakeholder management.

> *"Trustwave's deep expertise in cyber incident simulation identified gaps in our response plan and improved our ability to respond to a potential incident."*
>
> Health Services Provider

Trustwave®

©2022 Trustwave Holdings, Inc