CASE STUDY

Crisis Management: A Best Practice Approach in Healthcare

The proliferation of technology across industries has created immense opportunities as more and more data become readily available. With this at their disposable, business leaders can make impactful decisions that can lead to streamlined processes and new revenue streams. But as new technology is introduced, the attack surface expands from a cybersecurity standpoint. Digital marauders have become increasingly sophisticated, crafting new ways to siphon sensitive business data and disrupt processes, at times leading to physical damage by jeopardizing support systems and medical technology that's critical in the healthcare industry. Given the evolving threat landscape, the perimeter defense approach of yesteryear is no longer a viable option for organizations.

Trustwave®

Client Spotlight

This private Hong Kong hospital prides itself on personalized patient care, as well as state-of-the-art medical units and research and development (R&D) facilities. Given the sensitive nature of its work, the hospital quickly recognized the gaps in its crisis management playbook and decided to take action.

The Challenge

There's a lot at stake for organizations that operate in the healthcare realm. For a hospital that conducts R&D, a cyber attack could result in stolen sensitive data of significant commercial value. It could also mean stolen patient data, which is worth plenty in the cybercriminal underground. But the most costly consequence would be any affected hospital systems that could cut off access to databases and halt operations and jeopardizing patient welfare.

In contrast to physical threats, cyber attacks can be carried out from almost anywhere in the world, so attackers are often never identified. This makes crisis management especially challenging for organizations that manage vast amounts of disparate. But when it's information and systems that are tied to a human's well-being, restoring systems is a matter of life and death.

Industry Threat

According to the 2019 Trustwave Global Security Report, half of cyber attacks impacting healthcare organizations are aimed at compromising their internal networks. For any of these institutions, simply re-engaging the systems in place would not resolve the incident until the source of the attack is pinpointed and eradicated. The impact on the operations of the hospital could be catastrophic, so every measure should be taken to identify the source of compromise. Given the speed at which organizations operate today due to initiatives tied to digital transformation, it can be challenging to prioritize the slew of tasks related to risk management and incident response plans. Many organizations place these responsibilities on their IT departments when, in fact, data security requires a more strategic approach that includes not just technology, but also processes and people.

The Solution

Backed by its ample experience helping many organizations in the healthcare sector, Trustwave designed a custom tabletop drill exercise involving a fictional breach of the hospital's digital systems. As events escalated, the hospital's management team put their heads together to consider ramifications at each stage of the attack, supplemented by learnings from recent case studies on similar breaches. What emerged were clear directions for strengthening the hospital's crisis management protocols to achieve three key objectives:

- Engage in proactive risk management;
- Enrich the hospital's incident response and escalation capabilities; and
- Formulate actionable corporate crisis communication strategies.

Following the exercise, the management team concluded that taking a proactive stance would involve shifting the company's current position on data security, whether that means flagging suspicious links—even from known senders—or investigating all potential cyber threats, no matter how remote.

The exercise also highlighted the importance of incident response and escalation procedures in the event of a cyberattack, including formal processes for verifying threats, identifying the quantum of damage, and limiting the risk of lateral cyberattacks.

By bringing the hospital's management team together, Trustwave demonstrated how proactive cyber crisis management requires the involvement of all hospital departments – not just IT. Through this tabletop exercise, the senior executives gained a clearer understanding of the elements of a robust cyber crisis response and management plan, enabling the hospital to bring its standard of care even higher.

Trustwave®

©2018 Trustwave Holdings, Inc