MEDIGATE

Risk Management Overview

Understanding the Gaps in Risk Management

Solution Overview

Healthcare has a target on its back. Health IT Security reported a 45 percent spike in attacks against healthcare providers since November, as the sector accounted for 79 percent of all reported data breaches in 2020. This makes it more important than ever for health systems to get a handle on and take appropriate steps to minimize the risks to their assets and ongoing operations.

Given the complexity of clinical settings, which contain an ever-expanding number of devices, protocols, and workflows involved in the HDO's efforts to deliver real-time, high-value care, there is a lot that goes into understanding and managing risk. For each health system, there is a unique combination of people, processes, and technologies that need to be in place to ensure appropriate governance and risk mitigation efforts that align the organization's desired business outcomes.

Unfortunately, a lack of visibility, communication, and coordination between all the security, biomedical, clinical engineering, and business stakeholders within the HDO creates gaps in risk management programs that leave health systems vulnerable to exploitation and disruption. These gaps must be identified and closed if the health system is to establish a security stance for their clinical settings in line with their tolerance for risk.

Medigate Fills the Gaps

Medigate can help organizations create a comprehensive clinical device risk management program that will enable HDOs to establish and maintain acceptable risk levels. By providing a single source of truth for medical, IoMT, and IoT devices, the HDO's stakeholders can come together to effectively manage and secure their operations, from the edge to the core.

The Medigate Device Security Platform (MDSP) has redefined what clinical network visibility means. Acting as a continuous monitor, Medigate provides the granular device details and insights HDOs need to inform their risk management strategies. With extensive integrations and auto-generated

device- and vulnerability-specific remediation instruction-sets and security policies, HDOs have the vetted capabilities they need to strengthen their stance and maintain acceptable levels of risks throughout their clinical settings.

Accurately Assess Device Risks

Risk management frameworks that organizations traditionally rely on to guide the development of their risk management programs, such as NIST, lack the clinical context needed to make them effective in a healthcare setting. Medigate uniquely combines cybersecurity expertise with a deep understanding of medical, IoMT, and IoT devices, communication protocols, and clinical workflows to create an effective, clinically contextualized risk assessment framework for the connected devices in an HDO's network. These risk scores support the prioritization of remediation and mitigation activities that will help the HDO appropriately address risk in their environment. To learn more, please check out this infographic.

Manage Vulnerabilities

Medigate considers risks within the clinical context in which they exist, analyzing the devices within the HDO's clinical setting to identify and then recommend how best to address the vulnerabilities and potential threats these devices introduce. In addition to general indicators of compromise (IoCs) and common vulnerabilities and exploits (CVEs), Medigate monitors manufacturer alerts to uncover devices in the environment that could be open to exploitation.

Combining this information with the clinical context of the device, Medigate can recommend appropriate mitigations and remediations to preserve the availability and integrity of the devices. Because many of these devices are involved in care, risks have to be managed much differently from traditional IT to ensure dependencies are respected and operations kept intact. Medigate provides the clinical lens needed to ensure vulnerability management is carried out swiftly and safely. To learn more, please check out how Medigate and Rapid7 are working together to manage vulnerabilities in clinical networks.

Maintain Good Clinical Cyber Hygiene

To maintain the health and prevent the spread of threats within clinical networks takes good clinical cyber hygiene. Medigate helps HDOs achieve the rigor they need to maintain acceptable risk levels. With the ability to discover, assess, and manage the cybersecurity risks that medical, clinical and other unmanaged connected devices, such as IoT, introduce to the clinical network, Medigate helps HDOs manage risk across their enterprise, drive security improvements, and optimize their asset management. To learn more, please check out this At-a-Glance.

Consistently Protect from the Core to the Edge (Clinics)

Medigate helps smart connected health systems large and small keep their operations and patient care operating as it should. With deployments in more than 500 sites around the world, from the smallest outpatient clinics to the largest inpatient care providers in the United States, Medigate's success helping care providers of all sizes and diversity connect with confidence is proven. To learn more, please check out this AAG for securing clinics.

Operationalize Risk Management Programs (Services)

Medigate works with certified partners to enable HDOs to establish and maintain a Managed Clinical Security Service Program (MCSSP) that effectively protects their medical and IoMT environments on an ongoing basis. Medigate powers clinical device security services that give HDOs the clinical context they require to understand and effectively address the risks within their environment. To learn more, please check out solution overview.