EINPRESSWIRE

BTR: Healthcare Leaders Weigh Surgical Containment to Counter Rising Cyber Risks

Vince Crisler, Celerium

SILVER SPRING, MD, UNITED STATES, August 1, 2025 /EINPresswire.com/ -- Healthcare organizations are facing a perfect storm of cybersecurity threats, as legacy systems, budget constraints, and an expanding attack surface make them prime targets for increasingly sophisticated cybercriminals. As a result, the sector's traditional defenses are no longer sufficient to match the capabilities of today's attackers, according to Vince Crisler, Chief Strategy Officer (CSO) for Celerium, a cybersecurity firm that specializes in automated, active network defense.

In a recent BizTechReports executive vidcast for journalists, Crisler — whose career spans military cybersecurity, the White House, and multiple startup ventures — laid out a stark assessment of the healthcare industry's cyber risk posture. He argued that the combination of outdated infrastructure, cultural resistance to security protocols, and resource limitations has made healthcare one of the most vulnerable sectors to ransomware and data breach attacks.

> It's not about having the biggest security budget — it's about making smart, targeted decisions."
>
> *Vince Crisler, Celerium*

But Crisler also offered a strategic blueprint for healthcare leaders seeking to adapt. His prescription centers on a concept known as "surgical containment" — a method for rapidly detecting and isolating attacker infrastructure while maintaining critical business operations. This approach shifts the conversation from prevention at all costs to resilience and intelligent risk management.

The Strategic Vulnerability of Healthcare Systems

“Healthcare is caught in a perfect storm,” Crisler said. “You have aging systems, limited security oversight on medical devices, and networks that are often not properly segmented.” These factors, combined with attackers’ high valuation of protected health information (PHI) and electronic medical records (EMR), create a lucrative target environment for cybercriminals.

Recent research confirms just how lucrative these attacks can be. The IBM 2024 Cost of a Data Breach Report identified healthcare as the costliest industry for data breaches for the 13th year in a row, with an average breach cost of $9.77 million — nearly double that of the next highest sector. This staggering figure underscores why attackers prioritize healthcare organizations in their ransomware and data theft campaigns.

Unlike many industries, healthcare’s mission-centric focus on patient safety and care delivery often sidelines cybersecurity considerations. Medical professionals prioritize clinical outcomes, sometimes at the expense of IT governance — a dynamic that Crisler described as a cultural challenge. “There’s a persistent tension between the business of care and the discipline of security,” he noted. “Doctors bring in revenue. Security is a cost center. That imbalance can make risk management conversations very difficult.”

Cultural Shifts and Executive Accountability

Despite the grim outlook, Crisler sees encouraging signs of change — particularly among healthcare executives beginning to recognize that cybersecurity is a board-level risk. “These leaders manage risk every day in clinical and operational contexts,” he said. “They are rapidly coming to the conclusion that they don’t need to be technologists to understand that cybersecurity is fundamentally a risk management issue.”

The pressure is growing. In 2024 alone, 67% of healthcare organizations reported being hit by ransomware, according to a Microsoft Security Insider report, with 53% of those paying ransom demands, averaging $4.4 million per payout. These figures show how ransomware attacks have become not only a technological concern but a financial and operational imperative for executive leadership.

Crisler’s advice: focus on understanding specific risks and prioritize investments that yield the greatest risk reduction per dollar spent. “It’s not about having the biggest security budget — it’s about making smart, targeted decisions,” he said.

Surgical Containment: From Concept to Operational Strategy

In response to the evolving threat landscape, Crisler’s team at Celerium has developed an operational approach called “surgical containment.” Unlike traditional isolation techniques — which often involve taking entire systems offline — surgical containment aims to precisely disrupt attacker infrastructure while allowing core business operations to continue.

“The difference is like amputating a limb versus using a scalpel,” Crisler explained. “We want to isolate the attacker’s ability to operate within your environment without shutting down your systems.”

This strategy relies on rapid detection and automated response mechanisms, leveraging data analytics to identify malicious outbound traffic in near real-time. Rather than manually unplugging affected systems, organizations can use firewall integrations to block attacker-controlled IP addresses or command-and-control infrastructure, often within minutes of detection.

Surgical containment complements, rather than replaces, existing security operations by overlaying on top of current infrastructure — typically by integrating with perimeter firewalls. The approach allows even resource-constrained organizations to gain visibility and control without significant upfront investment.

The Role of AI and the Fight Against Alert Fatigue

While Crisler is skeptical of overhyped AI claims in cybersecurity offerings, he acknowledges its role in enhancing detection and response efficiency. Celerium applies AI and machine learning in targeted ways, such as improving dashboard readability with natural language generation and refining anomaly detection through advanced analytics. It can play a major role in addressing of the most acute challenges in cybersecurity: alert fatigue.

Most healthcare security operations centers (SOCs) face an overwhelming volume of notifications that can paralyze teams. It highlights the need to streamline alerts that have been amplified by the much higher frequency of attacks enabled by AI. A 2024 Forescout report, for instnace, revealed that healthcare organizations experience serious breach incidents at least twice per day, with ransomware leading the threat landscape. Crisler’s approach seeks to filter threats through automated, intelligence-driven processes that emphasize known malicious infrastructure and cross-organizational threat sharing.

“If we can help you identify a real threat based on collective intelligence and allow you to act before it becomes a crisis, that’s a win,” he said.

Real-World Applications and the Healthcare Impact

Celerium’s deployment model is designed for speed and minimal disruption. By configuring existing firewall logs to send data to Celerium’s secure SaaS platform, organizations can implement the solution in as little as 30 minutes. This quick-start capability allows security teams — or even non-technical administrators — to begin seeing threat activity almost immediately.

Crisler noted that this model appeals to a wide range of healthcare organizations, from small clinics to large hospital systems. For organizations with mature SOCs, surgical containment serves as a front-line filter, reducing noise and allowing teams to focus on the most critical threats. For those without dedicated security resources, it provides a baseline level of protection that would otherwise be cost-prohibitive.

The Path Forward: Risk Ownership and Resilience

Technology alone, however, cannot solve healthcare’s cybersecurity challenges. Crisler stated that the most important first step is for executive leadership to take ownership of cyber risk as a critical business issue. This includes conducting honest assessments of risk exposure, aligning with recognized security frameworks, and engaging in realistic tabletop exercises to prepare for breach scenarios.

For organizations that rely on managed service providers (MSPs), Crisler advises due diligence to ensure those providers are enforcing strong security standards, such as mandatory two-factor authentication and incident response planning. “If your MSP isn’t pushing you on security basics, they’re not the right partner,” he warned.

Ultimately, Crisler believes the healthcare industry must adopt a mindset of resilience — operating under the assumption that breaches are inevitable and focusing on minimizing impact when they occur. “It’s not about eliminating risk,” he said. “It’s about managing it in a way that keeps your operations running and protects your patients.”

Click Here to Read a Q&A Based on this Interview.

Airrion Andrews
BizTechReports
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/835887638