EPIPHANY SYSTEMS

Cyber Risk Hunting for the Healthcare Industry

CHALLENGE OF CYBER DISRUPTIONS TO HEALTHCARE

Healthcare and clinical operations harbor many cyber risk conditions, due to system complexity and the sheer number of devices involved. Many of these risks go undetected...until it's too late.

That makes the healthcare industry vulnerable to ransomware, distributed denial-of-service (DDoS) attacks, and malware-induced equipment failures.

Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) worry most about the operational impact of such risks. Chief Medical Officers worry most about patient care and clinical technology.

The healthcare field needs a better way to understand risk conditions and their potential downstream impacts. More specifically, the industry needs a way to hunt for risks—and mitigate them—before a cyberattack occurs.

The impact of these risks can be significant or even catastrophic, including:

- Disruption of clinical operations and medical care
- Inadvertent data exposure and heavy fines for HIPAA violations
- Increase in avoidable hospital readmission rates—and high related costs
- Danger to patients using connected devices, like pacemakers and insulin pumps

HEALTHCARE BREACHES GROW DESPITE IT EFFORTS

IT organizations in healthcare do their best to improve cybersecurity with the tools at their disposal. They segment networks to isolate devices, use configuration management tools, and scan/patch vulnerabilities.

But these approaches focus on a limited number of technical issues, which account for only about one-quarter of all cyber risks. They do not fully cover wider-ranging problems with misconfigurations, permissions, data exposures, and simple IT oversights that cause security "drift."

Also, most security tools do not understand technical issues in context with their real-world impacts. So IT teams get bogged down in triage. Overwhelmed with alerts, security analysts cannot prioritize issues by the impact they might actually have on healthcare services. Analysts can only react to the latest tactical "fires," not proactively hunt for strategic risks that pose the grimmest consequences.

As a result, cyber attacks continue to proliferate—and succeed—in healthcare environments. Recent history is littered with examples: Petya, NotPetya, WannaCry, DDoS attacks, and escalating ransomware hacks during the COVID-19 pandemic.

POTENTIAL DISRUPTION OF CRITICAL WORKFLOWS

A big part of the problem is that finding risk conditions in healthcare environments is difficult. Many internet-connected systems and devices cannot be scanned, do not support software agents, and cannot interact with cybersecurity tools. If disrupted, such systems and devices can severely impact key workflows in healthcare and clinical operations. For example:

LABORATORY OPERATIONS: Labs rely on expensive equipment, including analyzers, centrifuges, mass spectrometers, serum separators, reagent systems, and robotic freezers. Cyberattacks affecting these devices could delay crucial test results, diagnostics, and surgery schedules. And damage from malware could require costly equipment repairs or replacement.

SATELLITE OFFICE OPERATIONS: Doctors' offices, ambulatory care centers, and other satellite medical sites pose added risks. They are outside the core health network's IT boundary, but they exchange data through electronic medical record (EMR) systems. An EMR could act as a conduit to deliver ransomware from the satellite to the core network. And a cyberattack could also disrupt the EMR system, causing severe service delays.

PATIENT PORTALS AND TELEMEDICINE: Increasingly, patients communicate with healthcare providers through online portals and mobile applications. They connect with the core health network virtually to access medical records, schedule appointments, and receive care through telemedicine. As with satellite office operations, these interactions increase the risks of EMR disruptions and malware transitions across the network.

HOME TELEMETRY: Many patients rely on remotely-monitored medical devices at home, like heart monitors, insulin pumps, infusion systems, and CPAP machines. But home networks are notoriously insecure. And a network hack could result in device failure, which could negatively impact health, cause readmission, or even result in death.

WHAT HEALTHCARE ORGANIZATIONS NEED

Healthcare organizations need to understand the potential impact of risk conditions on both business infrastructure and patients. Revenue and liability are at stake, as well as individual health outcomes.

> ***But healthcare providers can't afford extensive downtime to clinical operations to run vulnerability scans. And even if they could, scanning isn't foolproof, since, as noted above, formal "vulnerabilities" make up only about 25% of all risk conditions.***

Organizations also need to understand the contextual relationships between network nodes and how they interact. A risk that impacts one node could potentially spread to thousands of others.

Gauging contextual risk relationships is hard enough in a healthcare system, due to the vast number of network nodes. But it is even more difficult to quantify risks when they can multiply exponentially across the environment.

That is a big reason why adversaries are able to penetrate healthcare organizations to launch ransomware and other cyber attacks. They use undocumented, unknown paths to spread the attack across the infrastructure.

QUESTIONS HEALTHCARE ORGANIZATIONS SHOULD BE ABLE TO ANSWER

- Do we understand the potential entry points for an attack on our network?
- Where do ransomware and other attacks have the highest probability of entry?
- Do we understand the combinations of technical conditions that allow attacks to succeed?
- What is the likelihood that our mitigations will be effective in correcting these conditions?
- Do we understand how an attack can spread?
- Have we modeled the interrelationships of our assets throughout the environment?
- Do we understand which types of attacks have the highest probability of success?
- If an attack occurs, do we understand what mitigations would minimize the impact?

NEW RISK HUNTING TECHNIQUES REDUCE CYBER RISKS FOR HEALTHCARE

Epiphany Intelligence Platform™ lets organizations answer these kinds of questions. A Risk Hunting platform absorbs data from existing network, security, and domain sources. (Epiphany is agentless; it does not directly interrogate data sources, so it does not disrupt any processes or operations.)

Risk Hunting looks at the current state of all technical risks—including those common IT issues that cause security drift. Risk Hunting also analyzes how those risks could potentially migrate across network paths. And Risk Hunting integrates an understanding of the operational value of each node on the network.

That all translates into an ability to quantify cyber risk in context with what is most important to the organization. For healthcare providers, that means understanding what risks could cause the most damage to their businesses and patients—and how.

With this deeper understanding, healthcare organizations can prioritize defenses to better protect against the risk conditions that could make them vulnerable to cyber attacks.

Awareness powers protection.

Contact us today to get started with Epiphany.

Contact Us

ABOUT EPIPHANY SYSTEMS

Epiphany delivers world-class cybersecurity solutions for enterprises in every sector of government and industry, including the Fortune 500. We are dedicated to reducing technical and business risks through innovative technologies, including artificial intelligence and machine learning.

Our mission is to safeguard our clients' data, assets, and operations across the globe. We assess each client's unique needs and challenges to ensure that their risks are visible, managed, and mitigated. If it's connected, it must be protected.