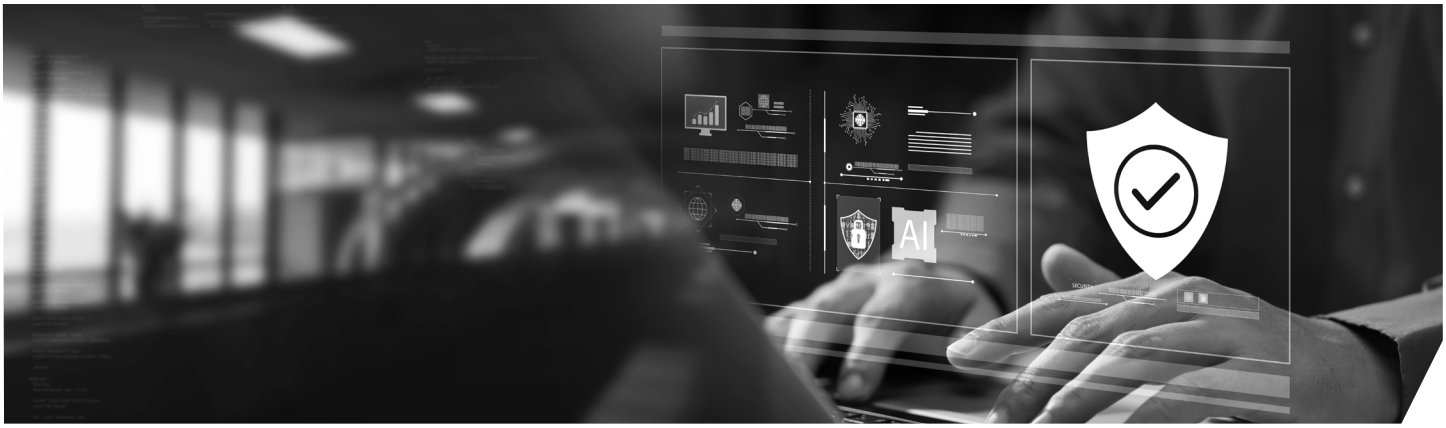
AMWINS

A Closer Look at Cyber Incidents in Healthcare

Recent media coverage of the alleged **Stryker cyber incident** has renewed attention on cyber risk across healthcare, life sciences and medical device manufacturing. While headlines often focus on attribution or worst case scenarios, events like this are not unfamiliar territory for cyber and healthcare risk professionals.

Rather than signaling a new or unprecedented exposure, incidents like this highlight why cyber risk management, cybersecurity controls and cyber insurance structures already exist, and why they have been refined over time. For organizations watching this situation unfold, the takeaway is not alarm, but preparedness.

03.26



How cyber insurance typically responds

Modern cyber insurance policies are designed to respond to a wide range of scenarios, including those that involve system destruction rather than data theft. While policy language varies by carrier, many share common coverage components; however, cyber policies are not standard ISO forms.

In events involving network intrusion and system disruption, multiple insuring agreements may be triggered, including:

- Incident response and forensics to determine how access occurred, what systems were affected and whether sensitive data was accessed
- Legal and regulatory support, especially if regulated data is implicated
- Public relations and crisis communications to manage stakeholder messaging
- Digital asset restoration, covering the cost to restore, recreate or replace lost or destroyed data

While these coverage elements have been part of cyber insurance since the product's early development and are not new additions in response to recent events, it is important to revisit them to help ensure that comprehensive coverage is in place.

Business interruption

For large organizations, especially those operating in the healthcare industry or manufacturing, business interruption is often the most significant source of loss following a cyber event.

Cyber business interruption coverage can address lost net income and certain extra expenses incurred while systems are down. This may include costs associated with relocating operations, outsourcing temporary services or accelerating recovery efforts.

Healthcare organizations and medical device manufacturers are particularly exposed because of the technology that supports nearly every aspect of their operations. When systems go offline, organizations may be unable to manufacture products, ship supplies, bill for services or access critical platforms. All these things can have immediate financial and operational costs.

Why is healthcare uniquely exposed?

Healthcare organizations face a dual cyber exposure that few other industries experience at the same scale. Highly regulated data and mission critical operations are large risks in this industry.

Healthcare systems, whether it be a hospital or a clinic, maintain vast amounts of sensitive patient information subject to strict regulatory oversight. They also rely heavily on interconnected systems to deliver care, manage prescriptions, schedule procedures, process billing and much more.

Medical device manufacturers face similar challenges. Supply chains, device software and operational platforms have become even more interconnected as medical technologies evolve at a rapid pace. A disruption affecting one link in the chain can ripple outward, affecting everyone from providers to patients and even downstream partners.

Practical takeaways for organizations

It's important that clients view cyber risk as a risk management discipline and not a transaction insurance purchase. Coverage is only one component of preparedness.

For organizations watching incidents like this, the most important steps are proactive rather than reactive:

- Regularly review cyber insurance coverage, including war exclusions and carve backs
- Evaluate business interruption and contingent business interruption exposures
- Assess vendor and supply chain dependencies
- Update and practice business continuity and incident response plans
- Understand Bring Your Own Device (BYOD) and device management exposures
- Review vendor contracts to ensure indemnification, limitation of liability and insurance requirements are clearly defined and aligned with cyber risk exposure
- Engage legal, risk and insurance teams early to negotiate vendor terms that meaningfully transfer risk and avoid coverage gaps

A plan that has never been tested for example, through tabletop exercises or scenario walkthroughs, is unlikely to perform effectively under pressure. Practicing those plans before an incident occurs can dramatically reduce confusion, downtime and downstream losses.

Takeaway

While incidents like the recent Stryker attack may attract attention, they do not represent a turning point for cyber risk management. Rather, they highlight why ongoing and proactive conversations with insureds are so critical. They also reinforce the fact that under the healthcare umbrella, cyber risk is a known and managed part of doing business.

When organizations do not fully understand the scope of their coverage and how it functions in a real-world incident, cyber events can be more intimidating than they need to be. Helping clients understand what their cyber policy does and does not cover, how business interruption exposure applies and where exclusions or sublimits may exist is just as important as placing the coverage itself.

As cyber risk continues to evolve, so too must coverage structures, contracts and internal controls. Ultimately, incidents like this are not a call for alarm, but a reminder of the value of informed partnership.

When clients understand their coverage, actively manage their risk and rehearse their response before an incident occurs, they are far better positioned to navigate disruption calmly and protect their operations, clients and employees.

We help you win

From ransomware and phishing scams to social engineering, cyber crime is constantly evolving. Amwins cyber specialists are entrenched in this business – leveraging their expertise, market relationships and broad network of colleagues across the U.S., London and Bermuda to secure the right coverage for your clients' needs.

Our exclusive **Cyber+ insurance program** combines tailored and enhanced coverage with industry-leading cyber security services. This exclusive product features comprehensive coverage with a broad appetite and best-in-class cybersecurity services.

Contact an **Amwins broker** today to learn more.

Insights provided by:

- Sarah Lambert, Divisional Director, Amwins Global Risk
- Augie Yost, VP, Amwins Brokerage

CONTACT

To learn more about how Amwins can help you place coverage for your clients, reach out to your local Amwins broker.

LEGAL DISCLAIMER

Views expressed here do not constitute legal advice. The information contained herein is for general guidance of matter only and not for the purpose of providing legal advice. Discussion of insurance policy language is descriptive only. Every policy has different policy language. Coverage afforded under any insurance policy issued is subject to individual policy terms and conditions. Please refer to your policy for the actual language.

Courtesy of Amwins Group, Inc.