Why Your Cyber Insurance May Not Be Providing You With The Cover You Really Need

Cyber insurance is increasingly recognised as essential for businesses in all sectors, but for UK life science companies, a standard policy may not provide the necessary protection. One critical gap lies in how most cyber policies are triggered: they focus on **financial losses**, often overlooking the potential for **bodily injury** caused by a cyber incident.

The Financial Trigger vs. Bodily Injury Risks

Traditional cyber insurance policies are designed to respond to financial losses, such as revenue drops, fines, or ransom payments, following a cyberattack. However, for life science businesses—especially those in biotech, pharmaceuticals, or medtech—the stakes are far higher. A cyber breach in this industry can result in:

- **Compromised clinical trial data**, impacting drug safety and approval processes.
- **Tampering with medical devices**, potentially causing harm to patients.
- **Disruption to manufacturing systems**, leading to defective products that may harm end users.

These scenarios go beyond financial loss, creating risks of bodily injury or even loss of life. A standard financial-triggered cyber policy may not respond to these claims, leaving businesses exposed to significant liabilities.

Specialised Risks Require Tailored Solutions

Life science businesses operate in a highly regulated environment where patient safety is paramount. A cyberattack that interferes with medical devices, disrupts clinical trials, or corrupts research data could have severe implications for patients and expose the business to legal or regulatory action.

What to Look for in a Cyber Insurance Policy

When evaluating cyber insurance, life science businesses should seek coverage that specifically addresses:

1. **Bodily Injury and Property Damage**: Policies should cover liabilities resulting from physical harm to individuals or damage to property caused by cyber incidents.
2. **Regulatory Support**: Protection for legal costs and penalties related to breaches of medical regulations or GDPR.
3. **Loss of Income and Extra Expenses:** Cover for expenses to recover or reconstruct critical data, including research data, patient information, or intellectual property. Losses arising from cyber incidents that prevent the company from conducting research, manufacturing, or delivering services.
4. **Specialist Incident Response**: Access to forensic, legal, and PR experts with experience in the life sciences sector.
5. **Tailored Exclusions**: Policies that explicitly include risks tied to medical device failure or disrupted manufacturing processes.

Avoid the Coverage Gap

Relying on a standard cyber policy may lead to significant coverage gaps, especially in scenarios where patient safety is impacted. Working with MFL Insurance Group Ltd, we can help you navigate these complexities and secure a policy that aligns with the unique risks of your business.

Life science SMEs must ensure their insurance strategy evolves with the growing interconnectivity of their operations. The right cyber policy not only protects your finances but also safeguards the lives and health of those who depend on your work.

For more information please contact:

Mark Philmore ACII, Chartered Insurance Broker
Client Director
Email: mp@mflinsurance.com
Direct Dial: 0113 323 1042
Mobile: 07966 233287