



The Cyber Coverage Gap: When General Liability and Cyber Insurance Don't Meet

Damion Walker, Managing Director
Gallagher Technology Practice



As organizations become increasingly reliant on connected technologies, cyber incidents are no longer limited to data breaches and privacy concerns. A cyber event can disrupt operations, damage equipment, impact critical infrastructure or contribute to bodily injury. At the same time, insurance carriers continue to refine where cyber-related losses belong within an insurance program.

This has created an important consideration for technology companies and other organizations that rely on connected systems: the potential gap between general liability and cyber insurance coverage.

Understanding how these policies work together can help organizations better assess their exposure and avoid unexpected coverage concerns when a loss occurs.



Why insurers are separating cyber risk

As cyber incidents have become more frequent and complex, insurers have increasingly sought to define which policies are intended to respond to specific types of losses. Stand-alone cyber insurance has evolved to address exposures such as data breaches, ransomware attacks, privacy liability, network security failures and other technology-related risks. Meanwhile, traditional liability policies were not designed to provide dedicated cyber coverage.

For many organizations, this distinction makes sense. Cyber insurance provides specialized coverage and response resources tailored to today's threat landscape. However, as coverage responsibilities are divided among different policies, it becomes increasingly important to understand where one policy ends and another begins.

How cyber exclusions are changing general liability coverage

Many general liability insurers now attach cyber incident exclusion endorsements that remove coverage for losses arising from cyber-related events. Depending on the endorsement's wording, exclusions may apply to claims involving:

- Data breaches
- Privacy violations
- Loss, corruption or unauthorized access to electronic data
- Network security failures
- Related liabilities and defense costs

These endorsements are becoming increasingly common across the insurance marketplace and may significantly narrow how a general liability policy responds to cyber-related incidents. Certain endorsements can also contain broad causation language that may affect coverage even when a cyber event is only one contributing factor to a loss.

While policy wording varies, organizations should review any cyber exclusion endorsements carefully and understand their potential impact on overall coverage.





The other side of the equation: Cyber insurance

Most stand-alone cyber and technology Errors & Omissions (E&O) policies are designed to address financial losses associated with data, networks, privacy obligations and business interruption. As a result, they commonly exclude bodily injury, death and physical damage to tangible property.

The reasoning is straightforward: Physical injuries and property damage have traditionally been handled by other insurance lines that are specifically underwritten and priced for those exposures.

However, some cyber insurers offer limited carve-backs or endorsements that may help address certain situations, including:

- Emotional distress arising from a data breach
- Damage to owned hardware resulting from a cyber event
- Specialized cyber-physical coverage enhancements

Because these provisions vary by carrier and policy form, organizations should review available options carefully.

Where coverage questions can arise

The greatest area of concern is often cyber-physical risk, where a cyber incident produces a real-world consequence in the form of bodily injury and/or property damage.

Examples can include:

- Ransomware disrupting a manufacturing operation
- A compromised building management system affecting facility functions
- Connected medical devices impacted by unauthorized access
- Industrial control systems operating outside intended parameters
- Technology failures that contribute to equipment damage or operational disruption

As technology becomes more deeply embedded within physical operations, products and infrastructure, these scenarios are becoming increasingly relevant for many organizations.

When a general liability policy excludes cyber-related incidents and a cyber policy excludes bodily injury or property damage, organizations may face uncertainty regarding how, or even whether, coverage would respond to a particular claim. While every situation depends on the specific facts and policy language involved, this overlap is an area that deserves careful attention.

Five Steps To Review Your Coverage

Organizations can take several practical steps to better understand how their insurance program responds to cyber-related incidents.

1 Review your general liability policy

Determine whether a cyber incident exclusion endorsement has been added and identify the specific form being used.

2 Understand the endorsement language

Not all exclusions are identical. Review the endorsement wording carefully and understand how it may affect coverage for cyber-related claims.

3 Review general liability and cyber policies together

Rather than evaluating each policy independently, review them side by side to understand how coverage responsibilities align and where gaps may exist.

4 Explore available coverage enhancements

Discuss available endorsements, carve-backs and cyber-physical coverage solutions that may be appropriate for your organization's operations.

5 Assess connected operations

Organizations involved in manufacturing, industrial controls, medical technology, critical infrastructure or connected products should pay particular attention to cyber-physical exposures and consider a more detailed review.



Frequently asked questions

What are cyber exclusion endorsements?

Cyber exclusion endorsements are general liability policy provisions that remove or limit coverage for losses arising from cyber-related incidents, such as data breaches, privacy violations, network security failures or electronic data losses.

Does cyber insurance cover property damage caused by a cyber attack?

Many stand-alone cyber policies exclude physical property damage. Some insurers may offer endorsements or specialized solutions that address certain cyber-physical exposures, depending on the policy structure and insurer.

Do organizations need both general liability and cyber insurance?

For many technology companies and organizations with significant digital operations, general liability and cyber insurance serve different purposes. The goal is to ensure the policies work together effectively and align with the organization's risk profile.

What is cyber-physical risk?

Cyber-physical risk refers to situations where a cyber event results in a tangible real-world consequence, such as operational disruption, equipment damage or bodily injury involving connected systems.

Making sure your policies work together

The addition of a cyber exclusion endorsement does not necessarily mean an organization's insurance program is inadequate, but in certain circumstances, it may indicate a significant coverage gap. It also highlights the importance of reviewing coverage as part of a coordinated risk management strategy.

As technology becomes increasingly integrated into physical operations, organizations should evaluate not only their cybersecurity controls but also how their insurance program responds when a cyber event leads to real-world consequences. Reviewing general liability and cyber insurance together can help identify potential coverage gaps, clarify expectations and support a more comprehensive approach to protecting the organization and its balance sheet.