Gallagher

Insurance | Risk Management | Consulting

Cyber-Physical Risks:
Addressing Coverage Gaps in Traditional Insurance

Property

Cyber-Physical Risks: Addressing Coverage Gaps in Traditional Insurance

Cyberthreats are no longer confined to data breaches and digital disruptions — they possess the potential to cause physical damage to your organization's property. With businesses becoming increasingly reliant on automation and interconnected systems to enhance efficiency, the risk of cyber incidents triggering physical damage is growing.

However, many traditional insurance policies might not adequately cover these risks, leaving organizations potentially exposed to costly financial and operational setbacks. Understanding coverage gaps and implementing proactive risk management strategies is crucial to safeguarding your assets against the evolving cyberthreat landscape.

The Hidden Risks in Traditional Insurance

Traditional cyber insurance primarily focuses on digital threats, such as data breaches and ransomware attacks, but typically excludes physical damage from cyber incidents. This leaves organizations vulnerable to financial and operational losses, particularly for sectors relying on Operational Technology (OT) environments.

A cyber attack targeting OT systems can have real-world consequences, such as equipment failures, production halts and infrastructure damage. From a health and safety perspective, physical damage attacks also have the potential to cause bodily injury.

In tune with these emerging threats, Property and Casualty (P&C) insurers have begun more explicitly defining cyber-related coverage within their policies. However, instead of expanding protection, many insurers are adopting broad, exclusionary language that significantly limits coverage for physical perils such as fire, explosion and flooding caused by cyber incidents.

As a result, organizations may unwittingly operate with critical coverage gaps, leaving them exposed to substantial financial losses in the event of a cyber-physical incident.

Cyber Attacks With Physical Consequences

The convergence of cyber risk and physical damage is becoming increasingly evident, particularly in industries that rely on OT, including but not limited to Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems. Sectors such as manufacturing, energy, transportation and hospitality are particularly vulnerable, as their operations necessitate complex digital systems that, if compromised, can lead to severe disruptions, financial losses and even personal injury.

In the hospitality sector, for instance, a cyber attack on a building management system could activate sprinklers, leading to significant water damage, business disruption and financial losses. Similarly, in manufacturing, hackers targeting ICS networks could override safety protocols, leading to machinery overheating, fires and production halts — endangering workers while resulting in property damage and business interruption.

For insureds in the energy sector, as an example, in a cyber attack on an offshore oil rig's control system, attackers could gain unauthorized access to the rig's industrial control systems (ICS) by exploiting vulnerabilities in the network. Once inside, they could manipulate the rig's operational parameters, such as altering pressure levels or shutting down safety systems. This manipulation could lead to physical damage, such as a blowout or spill, due to the inability to maintain proper control over drilling operations. The consequences could include environmental damage, financial losses and potential harm to personnel.

Cyber Exclusions in P&C Insurance

The rise in high-profile cyber incidents, such as the WannaCry and NotPetya attacks, has reshaped the way insurers assess and manage their exposure to cyber-related losses. These large-scale events demonstrated the potentially systemic consequences of cyberthreats. The widespread disruptions and spillover from such attacks have now prompted P&C insurers to implement a more cautious and restrictive approach toward covering cyber risks.

As a result, some P&C carriers have introduced absolute cyber exclusions in their policies, explicitly excluding any losses linked to a cyber event, regardless of the nature or impact of the attack. This shift has left businesses without affirmative cover for damages stemming from cyber incidents, even though these incidents lead to tangible physical consequences.

Other insurers have opted for more nuanced exclusions, differentiating between malicious and non-malicious cyber acts. In some instances, they provide limited carve-backs for named perils, such as fire or explosion, when directly triggered by a cyber event. However, these carve-backs often come with strict conditions — such as requiring robust cybersecurity measures, specific endorsements or proof of compliance with industry standards — and are typically offered on a sublimited basis, meaning that the coverage amount is significantly lower than the total policy limits.

Businesses that operate in sectors heavily reliant on OT face a significant challenge due to these exclusions. Unlike traditional IT-focused cyber risks, OT cyberthreats may cause direct physical harm, including equipment destruction, system failures and safety hazards, which may lead to bodily injury. The lack of clear coverage in P&C policies means organizations may face substantial uninsured losses, particularly as their standalone cyber insurance policies exclude physical damage claims.

Risk Mitigation Strategies: Strengthening Cyber and Physical Resilience

While insurance is a critical component of risk management, businesses must also take proactive steps to mitigate their exposure to cyberthreats, particularly those that could lead to significant physical damage or operational downtime. Key strategies include:

1 **Segregation of IT and OT environments**

OT systems were historically isolated from traditional IT networks. However, increased digitization and connectivity have blurred these boundaries, creating new attack vectors for cybercriminals. The expansion of the Internet of Things (IoT), for instance, offers cybercriminals potential doorways to access air-gapped systems.

Implementing strong segregation measures ensures cyberthreats targeting IT systems do not easily infiltrate OT environments, such as:

- Air-gapping
- Firewalls
- Strict access controls

By reducing interconnectivity where possible and applying stringent monitoring, organizations can minimize the risk of widespread cyber incidents affecting physical operations.

> "Not all systems and data are equally valuable. Organizations must prioritize their cybersecurity investments accordingly. By identifying their "crown jewels" — such as proprietary manufacturing processes, intellectual property or critical control systems — businesses can implement targeted protections for their most valuable assets."
>
> **Joe Stubbings, Director, Cyber - UK**

2 **Enhanced cyber hygiene and threat detection**

Cyber hygiene is the foundation of a strong security posture. Organizations should invest in:

- **Endpoint Detection and Response (EDR) tools:** These tools provide real-time monitoring and automated responses to suspicious activity on network endpoints, preventing cyber attacks before they escalate.
- **Security Operations Centers (SOCs):** A centralized SOC enables continuous threat detection and response, allowing businesses to swiftly identify and mitigate potential cyber intrusions.
- **Regular patching and updates:** Numerous cyber incidents exploit unpatched vulnerabilities. Ensuring all software, firmware and operating systems are regularly updated helps close security gaps.
- **Multi-Factor Authentication (MFA):** Restricting access to critical systems based on user roles and enforcing MFA reduces the risk of unauthorized intrusions.

3 **Incident response planning and crisis management**

Cyber incidents can still occur even with the best preventive measures in place. A sound incident response plan ensures that businesses can quickly detect, contain and recover from an attack, minimizing financial and operational disruptions. Key elements include:

- **Ransomware preparedness:** Establishing protocols for identifying and isolating infected systems, assessing ransom demands and determining whether restoration from backups is feasible.
- **Tabletop exercises and simulated attacks:** Regularly testing incident response plans through simulations helps employees and security teams practice their roles in real-world scenarios.
- **Cross-functional response teams:** Cyber incidents impact multiple departments — a coordinated approach can ensure swift decision-making and clear communication with stakeholders, regulators and customers.

In a world where cyberthreats continue to evolve, organizations that take a proactive stance will be better positioned to safeguard their operations, reputation and bottom line. By combining these strategies, businesses can strengthen their cyber and physical resilience, reducing their reliance on insurance as the sole means of protection.

Gallagher's Solution

Businesses must carefully review their insurance policies to understand potential coverage gaps as cyberthreats continue to grow in complexity. In some cases, companies may need to explore specialized insurance solutions to ensure adequate protection against cyber-induced physical losses.

Gallagher is at the forefront of providing innovative solutions to address these potential coverage gaps. Gallagher offers customized and enhanced cyber insurance solutions designed to protect organizations against these evolving threats. With the Gallagher team's expertise, businesses can effectively manage and transfer risks related to cyber-induced physical damage, business revenue loss resulting from such events and even bodily injury caused by cyber incidents.

Our recommended, all encompassing approach provides affirmative coverage for both physical and non-physical cyberthreats

A writeback solution, through which we can carve back cyber exclusions on P&C lines, to cover the physical impacts of a cyber incident

"Traditional" non-physical cyber insurance, which doesn't cover physical damage, PDBI or bodily injury

The table below outlines the non-physical damage and new physical damage cyber insurance solutions available:

Insuring module	Cyber non-physical and physical damage	Cyber property damage writeback	Cyber non-physical damage
Physical damage	X	X	
Business interruption arising from physical damage events	X	X	
Bodily injury	X	X	
Breach response costs	X		X
Security and privacy liability	X		X
Regulatory fines and penalties	X		X
Non-physical damage business and dependent business interruption	X		X
Digital asset restoration costs	X		X
Cyber extortion	X		X
PCI DSS assessment	X		X

Contact Gallagher today to learn more about our specialized solutions and ensure your organization is protected against physical damage caused by cyber incidents.

Joe Stubbings
Director
Technology & Cyber Practice — Financial and Professional Risks
M: +44 (0)7825 439 723
E: joe_stubbings@ajg.com

Will Slater
Executive Director
Technology & Cyber Practice — Financial and Professional Risks
M: +44 (0)7843 068648
E: will_slater@ajg.com

AJG.com **The Gallagher Way.** Since 1927.

Gallagher