January 2026 - Safety Bulletin

Cyber and Data Vendor Risk Transfer Considerations

Vendor Limitation of Liability: Key Considerations

When engaging with cyber and data vendors, it is common practice for these vendors to attempt to limit their liability to the total value of the contract. However, this approach does not adequately reflect the true risk exposure faced by the insured member. It is essential for members to thoroughly assess the extent of data the vendor will access, the methods by which this data is accessed, and the potential financial impact of a data breach involving that vendor. In most cases, the contract value is not a reliable indicator of exposure. Therefore, the limitation of liability should instead correspond with the required cyber liability coverage and limits.

Professional Services Agreements and Standard Risk Transfer Methods

Members should ensure that they utilize their professional services agreements when retaining vendors who provide services. Standard risk transfer methods must be incorporated into these agreements. These methods include requirements for general liability insurance, workers' compensation, commercial auto coverage, indemnity provisions, and naming the member as an additional insured. Additionally, cyber liability coverage must be in place where certain exposures are present.

Situations Requiring Cyber Liability Coverage

- Data Handling: If a vendor is responsible for any sensitive or personal data—including names, addresses, social security numbers, medical records, or financial information—cyber liability coverage is essential.
- System Access: Vendors or contractors with access to your network or systems, or those who process, manage, or store data on your behalf, necessitate cyber liability coverage.
- Industry-Specific Risks: Certain industries, such as healthcare, financial services, and technology service providers, have higher exposure and should be contractually required to carry cyber coverage.
- Mission Critical Vendors: Even when sensitive data is not involved, business disruption caused by a cyber-attack on a vendor can result in significant damages to daily business operations.
- Compliance and Regulatory Requirements: Regulations such as Health Insurance Portability and Accountability Act, General Data Protection Regulation, and Payment Card Industry Data Security Standard require robust risk management practices, which can be supported through the inclusion of cyber liability insurance.
- Contractual Obligations: Cyber liability insurance should be included whenever required by contract.
- Consideration of Potential Damages: Evaluate whether a cyber-attack could cause substantial financial harm to your business or lead to significant damages that disrupts the vendor's operations.

Technology vendors may seek to restrict their indemnification obligations to the contract value. This limitation is not always appropriate and should be carefully reviewed by your legal team.

Technology Errors and Omissions (E&O) Coverage

- When Tech E&O Is Necessary: If your organization relies on external technology experts for advice or services, any mistakes on their part could result in financial loss or disruption to your daily activities.
- Contractual Requirement for Specific Businesses: Businesses involved in the development or implementation of critical software, IT consulting or services, website design, and cloud computing should be contractually required to carry Technology E&O coverage.
- Coverage of Gaps: Tech E&O insurance can address gaps left by general liability and cyber liability policies.
- Protection for Mistakes: This coverage provides protection against inadvertent errors and omissions.
- Financial Protection: Tech E&O can cover legal costs, settlements, and judgments arising from lawsuits related to the vendor's technology services.

It is important to note that large technology vendors often attempt to limit their indemnification obligations to the value of the contract. Such limitations may not be suitable and should be reviewed by your legal team.

For more detailed information, refer to the Contractual Risk Transfer Manual – Chapter 4.

If you have questions about either of these programs contact Bob May, Director of Loss Control. Phone – 760.221.8205 or biem47@outlook.com