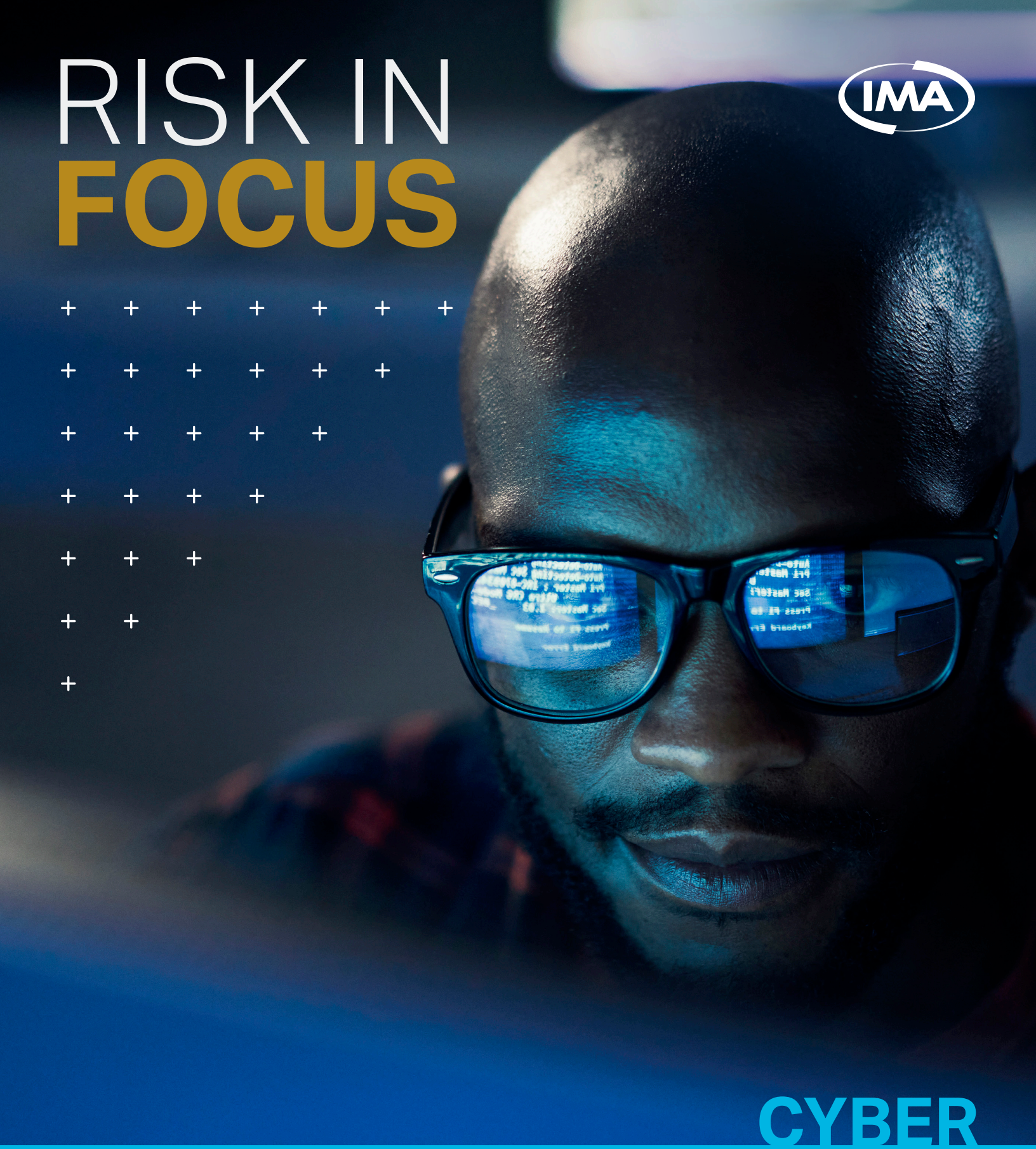
RISK IN FOCUS



CYBER

Managing Cyber Supply Chain Risk

Q2 | 24

INTRODUCTION

An organization faces cybersecurity risks at several junctures in its supply chain, including risks stemming from a vendor's cybersecurity missteps or misfortune. This risk was very apparent recently when a cyberattack against a single company affected operations at a large number of healthcare businesses.

TABLE OF CONTENTS

Overview

A ransomware attack against Change Healthcare in February 2024 caused a system shutdown lasting more than a month. Change provides electronic infrastructure for payments and other matters to healthcare providers, pharmacies, and other healthcare businesses. Change is widely used in the industry, and its shutdown prevented its customers from issuing bills, receiving payments, issuing electronic prescriptions, and performing many other functions.[1] Many healthcare providers experienced significant financial hardship and impact on their businesses.

As the Change Healthcare attack demonstrates, supply chain cyber risk can affect an entire industry. The level of supply chain cyber risk is rising, too, as companies increase their reliance on third parties to supply essential goods and services that depend on the functionality of the vendors' information and operational technology systems. Cyber attackers know all too well that breaching the IT systems of a key vendor such as Change Healthcare can create enormous disruption to many other companies. That fact can give a threat actor immense leverage in an extortion situation.

There are steps organizations can take to avoid becoming victims of their vendors' cybersecurity incidents or at least minimize the impact of these incidents. Those steps include enhanced review and verification of their suppliers' cyber risk controls and risk transfer strategies available through appropriate cyber insurance products.

Risk Mitigation

A company's risk management strategies should seek to ensure that its suppliers maintain appropriate procedures, policies, and standards. This should involve creating a cyber vendor risk management (CVRM) program. **A comprehensive CVRM program should include:**

+ **Identification of all vendors whose disruption could have a material effect on the company and/or its customers.**
+ **Attestations** – Note whether the vendor conforms with cybersecurity protocols laid out by organizations such as the American Institute of Certified Public Accountants AICPA), National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technologies (COBIT), International Standards Organization (ISO), and other reputable groups.[2]
+ **An assessment of the vendors' cybersecurity.** This is frequently accomplished through questionnaires built to align with the organization's cyber risk management goals and with the risks inherent in the functions the vendor is performing. The NIST offers a list of detailed questions that could be included in this questionnaire.[3] The questionnaires should be updated at least annually. Supplemental questions should be asked as new significant cyber vulnerabilities are identified.
+ **Continuous monitoring of vendors' cybersecurity.** The most effective way to do this is to use third-party cyber risk rating tools and others that can monitor specific vendors and provide relevant information to the organization. These can also help assess the cybersecurity of fourth parties (vendors of vendors).

DID YOU KNOW?

Many cyber insurance carriers provide complimentary scanning of critical vendors.

This pro-active approach can provide you with advance notice of any possible vulnerabilities at the vendor level.

- Contractual requirements for vendors regarding cybersecurity. **Those can include:**
  - Maintenance of specified levels of cybersecurity;
  - Indemnification of the organization for cyber incidents affecting the vendor;
  - Delineation of responsibilities between the organization and the vendor for investigation and other matters when a cyber incident takes place and
  - Maintenance of cyber insurance that will pay losses sustained by the organization resulting from a cyber incident affecting the vendor.

RISK IN FOCUS

Risk Transfer: The Role of Cyber Insurance

Risk transfer through insurance coverage is critical to a comprehensive risk management strategy. There are carefully designed insurance products that can protect a company from damaging fallout from cyber incidents in their supply chains.

- **Cyber Liability Insurance** – coverage for liabilities arising from a data breach or attack on an organization's computer system is commonly found in cyber policies. It isn't difficult to imagine how liabilities could arise from an organization's failure to protect information or deliver goods and services for a customer because of a cyber incident affecting a critical vendor. It is important to ensure that the coverage is broad enough to include such losses.
- **Contingent Business Interruption (CBI) Insurance** – CBI insurance, typically contained in a well-constructed cyber policy, covers loss of income because of a cyber incident affecting one of the organization's vendors. This coverage typically extends to fixed operating costs incurred while the organization's business was impaired, and costs to mitigate the loss.

CBI insurance coverage is widely available. Moving forward, organizations can expect underwriters to scrutinize the policyholder's vendor management and business interruption protocols related to:

- How well they vet the cybersecurity policies and practices of their vendors.
- How well does their business continuity plan adequately account for supply chain disruptions due to vendor cybersecurity breaches or other causes.
- Whether the insured's vendor contracts adequately address cybersecurity requirements and data breach notifications.

As more vendor cybersecurity events occur, policyholders may find that insurers want to limit CBI coverage. We have already seen insurers impose sublimits. We may see more drastic limitations if the Change Healthcare incident and others adversely impact cyber insurers' profitability.

The cyber insurance marketplace will continue to innovate and provide new risk transfer solutions. Parametric policies providing CBI coverage are one example. A parametric policy requires the insurer to pay an agreed-upon, fixed amount following confirmation of a specified insurable event. This could include, for example, a service outage suffered by a major cloud provider such as Amazon Web Services, Google Cloud, and Microsoft Azure.

A Final Word

Sound supply chain risk management is essential. Organizations must identify exposures and actively manage this rapidly evolving area of risk. Proactive controls such as CVRM and sound terms in vendor contracts will assist with mitigation. As with other areas of risk that carry substantial financial consequences, insurance-based risk transfer should be seriously considered.

IMA maintains a practice group with experienced professionals 100% dedicated to cyber risk management. Our team assists clients in coverage analysis, financial loss exposure benchmarking, contract language review, cyber threat analysis, and placing tailored cyber insurance programs.

MORE THAN JUST **INSURANCE**

IMA is an integrated financial services company specializing in risk management, insurance, employee benefits and wealth management. As an employee-owned company, IMA's 2,300-plus associates are empowered to provide customized solutions for their clients.

CONTACT THE IMA TEAM

For additional questions regarding this content or the resources that our carrier partners offer, please reach out to our Cyber Practice Leader.

TIM BURKE
EVP, Head of Cyber / Commercial E&O
303.615.7676 | *tim.burke@imacorp.com*

RISK IN **FOCUS** | CONTRIBUTORS

TIM BURKE, *EVP, Head of Cyber / Commercial E&O*

WILLIAM BOECK, *EVP, Cyber Product Leader*

ANGELA THOMPSON, *Marketing Specialist, Market Intelligence & Insights*

SOURCES

[1] U.S. Department of Health and Human Services. (2024, March 5). **HHS Statement Regarding Cyberattack on Change Healthcare.** *https://www.hhs.gov/about/news/2024/03/05/hhs-statement-regarding-the-cyberattack-on-change-healthcare.html*

[2] RiskOptics. (2022, August 22). **A Guide to Cybersecurity Attestation.** RiskOptics. *https://reciprocity.com/resources/what-is-cybersecurity-attestation/*

[3] National Institute of Standards and Technology. (n.d.). **Best Practices in Cyber Security Supply Chain Risk Management.** National Institute if Standards and technology. *https://www.nist.gov/system/files/documents/itl/csd/USRP_NIST-Utility_100115.pdf*

NPN 1316541 | IMA, Inc dba IMA Insurance Services | California Lic #0H64724