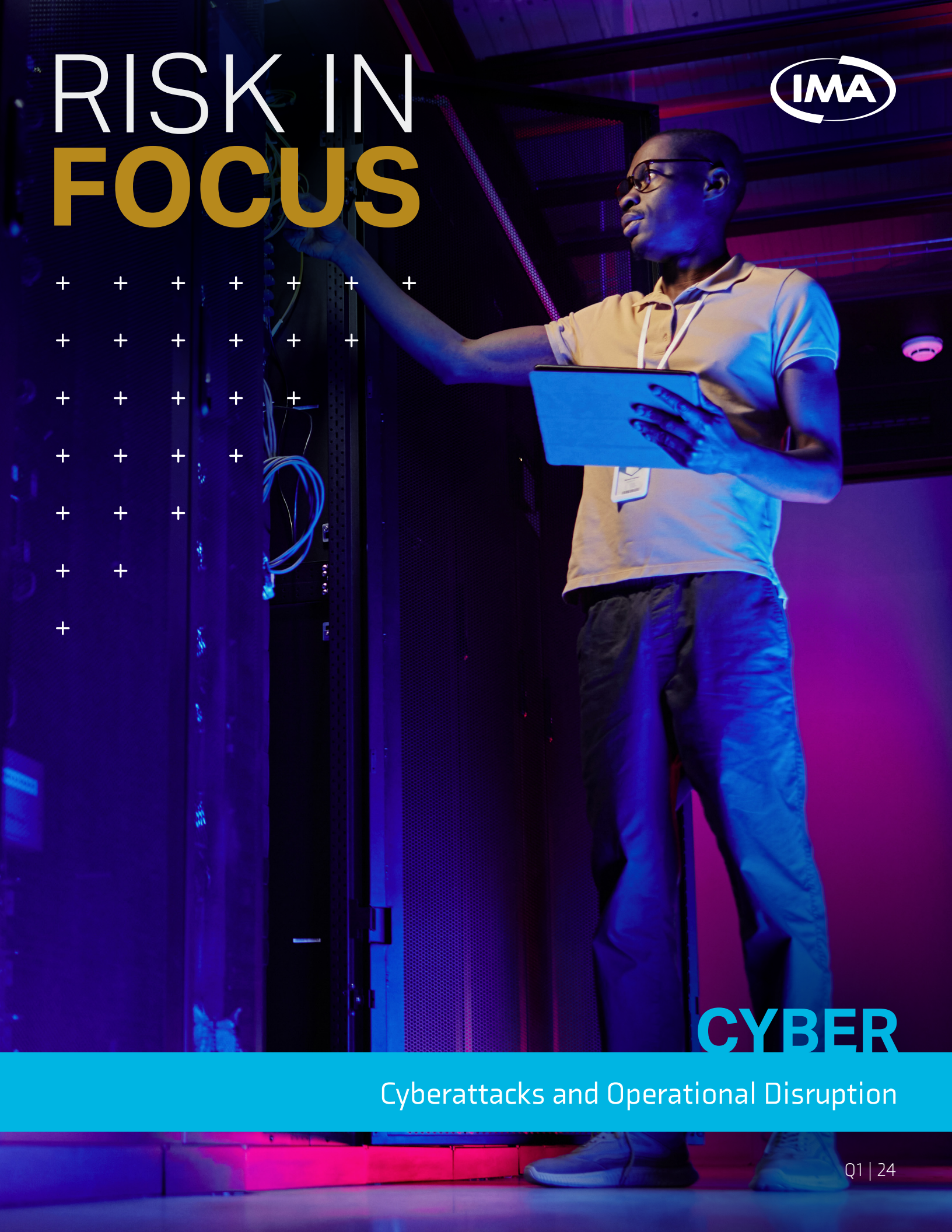
RISK IN FOCUS



CYBER

Cyberattacks and Operational Disruption

Q1 | 24

Introduction

Cyber risk is an evolving and often misunderstood class of risk. Rapid technological change, the ever-increasing reach and skills of hackers, and the unpredictability and often unexpected cost of cyber events compound the challenges and increase the stakes for cyber risk protection.

There are many varieties of cyberattacks. The most frequent are denial of service (DOS), data breaches, ransomware, theft of proprietary information, theft of financial resources, and disruption of supply chains. The common denominator in each of these is the disruption of operations within the organization. Short-term losses from ransom settlements and even financial cybertheft can pale in comparison to the long-term costs incurred due to an operational disruption.

TABLE OF CONTENTS

01 Operational Disruption

04 Cyber Insurance

05 A Final Word

Operational Disruption

Business operation disruption, with its inherent loss of productivity and revenue, is always a concern for business leaders. A recent study found that cyberattacks are considered the most likely cause of business disruption for leaders of companies of all sizes.[1] The financial costs can be significant.

These costs arise in various areas, and business leaders must identify both the possible and likely scope of potential impacts from an operational disruption in their company.

A recent analysis from Deloitte found that business leaders tend to gravitate toward calculating the more easily quantifiable costs from a cyber incident – the breach of customer and employee records, for example, along with legal judgments and penalties – and less on the costs related to more serious impacts, including the disruption of operations. Although these are more difficult to quantify, their cascading impacts represent a more severe threat to the business's long-term viability.[2]

Fortunately, there are models to estimate operational disruption costs and best practice recovery techniques, such as establishing Recovery Time Objectives and incident response plans for critical systems and applications. In combination, these steps enable business leaders to manage cyber risks more completely and plan for a stronger recovery.

OPERATIONAL DISRUPTION CASE STUDIES

CLOROX® COMPANY

The consumer-products giant Clorox® Company was the victim of a catastrophic cyberattack in Q3 2023, and Q1 2024 results suffered significantly: “Order processing delays and significant product outages” dented quarterly sales by 23-28%. That’s likely well over $500 million in lost revenue.[3]

SOUTHWEST AIRLINES

A network outage that hit Southwest Airlines in 2016 caused the cancellation or delay of more than 2,000 flights. The price tag was pegged at $82 million in increased costs and lost revenue — and that doesn’t consider the public relations impact nightmare and loss of goodwill. Southwest blamed a faulty router, which it says prompted a widespread network system failure.[4]

MANAGING CYBER RISK

Do we have an incident response plan (IRP) that addresses cyber events?

+ Have we stress-tested the IRP with a tabletop exercise?
+ Have we identified all critical vendors to assist us with response and recovery?
+ How are we handling communications with clients?

Do we practice proper cyber hygiene?

+ Multi-factor authentication
+ Endpoint detection and response
+ Secure backups
+ Network access controls
+ Patch management
+ Employee cybersecurity training
+ Secure remote access

Do we have good information governance practices?

+ Do we collect and keep information we don't need?
+ Do we keep information longer than necessary?
+ Is protected and/or sensitive information encrypted?
+ Do we limit access to information to only those with a need for it?

Have we considered and purchased cyber insurance?

+ Do we have adequate balance sheet protection for extended downtime?

PROTECTING AN OPERATION FROM A SUPPLIER'S DISRUPTION

Most organizations rely on third-party technology service providers for critical functions. For example, automated inventory systems and cloud-based collaboration platforms are deeply embedded into business operations. If a company's critical service provider is the source of a prolonged attack, this also can substantially disrupt the company's operations. Companies should account for this risk in their business impact analyses.

DID YOU KNOW?

Third parties cause 70% of all operational downtime, meaning companies cannot predict or control outages that may affect them.[5]

RISK IN FOCUS

Cyber Insurance

Cyber insurance was introduced more than 25 years ago to address new and emerging risks not contemplated in traditional Property & Casualty policies. While these cyber policies have evolved to address additional risks, at their core, they are like traditional insurance with similar coverage provisions, such as business interruption and property damage. **Some of the notable benefits include:**

FREE OR DISCOUNTED LOSS PREVENTION SERVICES

+ Confirmation if controls are in line with best practices
+ External scanning to provide proactive notice of vulnerabilities

RISK TRANSFER

+ Immediate triage resources upon discovery of an event
+ Access to technical investigation experts
+ Forensic accountants
+ Extra expense reimbursement
+ Fund expenses to re-create data
+ Indemnification for loss of income
+ Contingent business income loss due to a supplier's disruption
+ Specialized cyber policies can cover physical damage to property caused by a cyber event

RISK IN FOCUS

A Final Word

Information and operational technology advances will continue to drive scale and efficiencies, helping companies innovate and differentiate in their markets. Unfortunately, these rapid changes come with risks – most notably, the potential for operational disruption when they fail or are compromised.

This is the primary reason cyber risk is consistently ranked as an organization's top concern. The unknown volatility associated with disruption from a successful cyberattack can lead to substantial financial loss and, in the worst cases, bankruptcy.

Every organization should take a proactive approach to managing and measuring these emerging risks. Cyber insurance is now an essential corporate finance tool to assist with reducing this volatility. After all, cyber insurance is a blend of risk mitigation tools, a financial backstop, an information-sharing medium, and a source of predictive analysis.

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*
BRIAN LEUGS, *Writer*

SOURCES

[1] Allianz. (2024). **Allianz Risk Barometer 2024: Cyber Incidents.** Allianz. https://commercial.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2024-cyber-incidents.html.

[2] Mossburg, E., Gelinne, J., & Calzada, H. (n.d.). **Beneath the Surface of a Cyber Attack.** Deloitte. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf.

[3] Barsky, N. (2023, October 6). **Clorox Crisis Shows Cyber Risks' Harsh Business Downside**. Forbes. https://www.forbes.com/sites/noahbarsky/2023/10/06/clorox-crisis-shows-cyber-risks-harsh-business-downside/?sh=57a61384632b

[4] Global Data Vault. (n.d.). **Southwest Airlines Avoided $82M Disaster**. Global Data Vault. https://www.globaldatavault.com/blog/southwest-airlines-avoided-82m-disaster/#:~:text=Faulty%20Router,four%20full%20days%20to%20resolve

[5] At-Bay. (2023, June 30). **Understanding Contingent Business Interruption in Cyber Insurance.** At-Bay. https://www.at-bay.com/articles/contingent-business-interruption-cyber-insurance/

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