Aon Risk Solutions
Financial Services Group | Professional Risk Solutions

Entertainment & Hospitality
Cyber Risk Exposures and Solutions

Cyber risk refers to the loss potential an organization faces by virtue of its reliance on information technology, connectivity and automated processes. While improved efficiency is derived from technology implementation, organizations face additional risk from the cyber exposures inherent in technology systems. In an increasingly punitive legal and regulatory environment, and in the face of more frequent contractual requirements for cyber liability insurance, forward-thinking companies are taking proactive steps to explore and transfer cyber risk. Unlike many organizations that only hold customer data, most Entertainment & Hospitality companies are also concerned with exposures beyond privacy risk, including content creation or distribution risk.

Numerous factors contribute to an organization's cyber risk profile, including: actions by employees, system and program glitches, security measures, content review practices, nature and quantity of data collected, and political or headline risk.

Entertainment & Hospitality cyber concerns

- Organizations are responsible for the vast amounts of payment card information that flows through their systems and are subject to the rules and regulations of the Payment Card Industry and other regulatory bodies.
- Point-of-Sale systems (POS) are often targeted by bad-actors as the entry point into corporations' network.
- Frequent technological advances in the POS space create efficiencies in the payment process however open the door to new vulnerabilities to hacker.
- New mandates and standards (EMV chip-compliance) are frequently being introduced and oftentimes require immediate attention.
- Ongoing reliance on critical vendors to maintain operations
- Aggressive tactics by marketing to collect and monetize membership data without familiarity of regulatory landscape
- Acts of rogue employees to abuse corporate information
- Bad actors utilizing ransomware to exploit the company for a quick reward
- Interruption to systems / network resulting in loss of income and / or extra expenses

How do organizations transfer cyber risk?

- The cyber insurance marketplace provides service solutions, including loss control resources, data breach coaches, dedicated claims resources, pre-approved panels of vendors and service providers to address each element of breach response
- Breach response coverage offering varies based on insurer and policy structure
- 60+ insurers provide cyber coverage with large capacity available

We're here to empower results

If you have any questions about your specific coverage or are interested in obtaining coverage please contact your Aon broker or visit **aon.com.**

The Aon acquisition of **Stroz Friedberg** enhances the ability of Aon to support clients with leading digital forensics and incident response capabilities.

Empower Results®

Scope of cyber coverage available in the insurance marketplace

Third Party Coverage Elements

- **Media liability**: defense costs and damages suffered by others for content-based injuries such as libel, slander, defamation, copyright infringement, trademark infringement, or invasion of privacy
- **Security and privacy**: defense costs and damages suffered by others resulting from a failure of computer security, including liability caused by theft or wrongful disclosure of confidential information, unauthorized access, denial of service attack or transmission of a computer virus
- **Regulatory defense and fines**: defense costs for proceedings brought by a governmental agency in connection with a failure to protect private information and / or a failure of network security
- **PCI fines and assessments**: defense costs for investigations brought by the Payment Card Industry (PCI) in connection with a failure to protect private information and / or network security

First Party Coverage Elements

- **Breach response costs associated with**: breach notification, including the hiring of outside law firms and public relations consultants, forensic costs, credit monitoring / protection, notification hot-line / call center, identity theft resources
- **Network business interruption**: loss of income and extra expense due to network security failure
- **Dependent business interruption**: reimburses the insured for actual lost net income and extra expense incurred when the insured's IT service provider's computer system is interrupted / suspended due to a failure of network security
- **System failure**: coverage for business interruption due to an unintentional or unplanned system failure not caused by a failure of network security
- **Data restoration**: costs to restore / recreate data / software resulting from network security failure
- **Cyber extortion**: reimburses the insured for expenses incurred in the investigation of a threat and any extortion payments made to prevent or resolve the threat

Aon Cyber Innovation

The Aon Cyber Enterprise Solution is the first of its kind policy that broadens the scope of cyber coverage to include: property damage arising out of a network security breach, business interruption and extra expense coverage arising out of a systems failure, contingent network business interruption for IT vendors and the supply chain, cyber terrorism coverage, etc. This product provides catastrophic limit in excess of $400M USD.

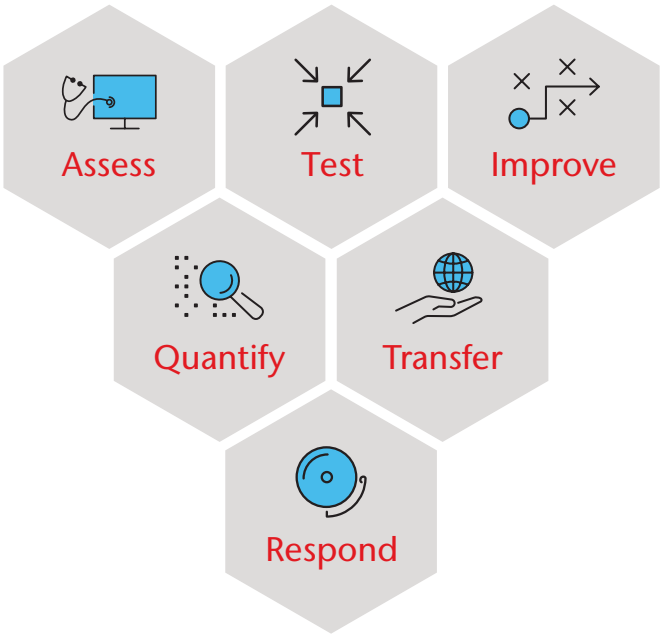
James C. Trainor joins Aon after a distinguished career at the Federal Bureau of Investigation, where he most recently led the Cyber Division at FBI headquarters. During his 20-year career with the FBI, he played a critical role in division strategies to combat ransomware and additional emerging forms of cybercrime, spearheaded major high-profile investigations, and managed numerous incidents at the nexus of cybercrime and national security.

Acquisition of Stroz Friedberg Aon's union with Stroz Friedberg provides a unique opportunity for Aon to build on our industry leading brokerage expertise, creating a comprehensive suite of assessment and quantification solutions to support our clients.

Darin McMullen hired to our Professional Risk Solutions practice. Darin is an E&O/Cyber Product Leader to focus on developing policy language with clients and Insurers, supporting clients and Aon's claims colleagues throughout claims negotiations, and working with our product development teams as we continue to innovate in this space. Darin joins Aon from Anderson Kill, a corporate law firm best known for its work in insurance recovery.

Aon Cyber Resilience Framework

Aligned with client's risk management approach to cyber security, Aon's approach helps identify and protect your critical assets and balance sheet by aligning your cyber enterprise risk management strategy with your corporate culture and risk tolerance. To achieve this, Aon recommends the following framework:



Empower Results®