Aon Risk Solutions

Cyber Risk Solutions for the Retail Industry

AON

Empower Results®

Aon Cyber Resilience Framework

In the world of cyber, resilience strategies help companies to rapidly detect, respond to, and recover from cyber threats and attacks. Aon has developed a Cyber Resilience Framework that addresses the cyber needs of our retail industry clients.

Assess

Identify critical assets, pinpoint vulnerabilities, and assess cyber preparedness to improve risk exposure

Aon Cyber Diagnostic Tool, Aon Cyber Coverage Gap Analysis, Aon Cyber 360° Suite of Solutions

Test

Uncover, test and remediate application, network and endpoint vulnerabilities

Aon Cyber Solutions Group Red Team Security Testing, Social Engineering Testing, Application Security Testing, Network & Cloud Penetration Testing and Configuration Review, Source Code Security Review, Threat Hunting

Improve

Prepare, optimize, and enhance security governance and incident detection and protocols

Aon Cyber Solutions Group Incident Response (IR) Retainer, IR Planning & Playbook, Tabletops, CISO/ Board Advisory

Quantify

Quantify the financial impact from cyber risks to inform risk reduction and transfer strategies

Aon Cyber Insight, Aon Cyber Impact Analysis, Aon Risk Financing Decision Platform

Transfer

Explore risk transfer solutions to minimize balance sheet risk

Aon Cyber Enterprise Solution, Aon Cyber Captive Program, Aon Proprietary Peer Benchmarking, Aon Client Treaty, Aon Benfield Reinsurance Capacity

Respond

Limit business disruption, minimize economic loss, and expedite the claims management process

Aon Cyber Solutions Group Incident & Breach Response, Aon Cyber Solutions Group Malware Reverse Engineering, Aon Claims Advocacy, Aon Business Interruption Claims Preparation

These pillars are supported by end-to-end solutions that span across Aon, including:

- Professional Risk Solutions (PRS): our dedicated cyber insurance broking team
- Aon Cyber Solutions Group: our leading cybersecurity professionals in proactive cyber resilience planning including digital forensics, incident response, due diligence, eDiscovery, and investigations
- Aon Global Risk Consulting (AGRC): our team focused on data and analytics, risk consulting, and alternative risk solutions

Why Retail Companies Should be Concerned About Their Cyber Risk Exposure

Cyber risk within the retail industry presents unique challenges. Privacy of customer credit and associated personal and health information are major risks; meanwhile, a host of technology vendors are supporting everything from e-commerce to in-store transactions to social media marketing. With high-profile industry breaches setting the standard and requirements for ongoing investment in cyber security and planning, it is no wonder that strategies to secure customer data, protect brand integrity, and respond effectively to incidents are on the minds of retail leaders.

Aon has been engaged in over 80 percent of the significant retail breaches to date. We have made significant investments into delivering a concise best practice approach to engage retail organizations in a roadmap to prevent, mitigate and manage cyber risk.

Aon is leading the industry with resources that can support a holistic view of cyber risk management. Aon's best-in-class teams and programs are designed using multi-disciplined perspectives that understand the responsibilities of risk management, finance, information technology, internal audit, human resources, operations and the c-suite. Aon understands that these disciplines must work together, without gaps or conflicts, and with documented validations that provide confidence that the strategies will deliver when an incident occurs.

Cyber exposure applies to retailers in many ways, including:

Data aggregation

- Potentially large amounts of consumer and employee data, including significant amount of credit card data being transmitted and/or stored
- Significant outsourced data and system partners
- Store credit card bank obligations and contracts
- Point-of-sale exposure

Regulation

- Payment Card Industry (PCI) Compliance
- International Organization for Standardization (ISO) Compliance
- U.S. Securities and Exchange Commission (SEC)
- Committee of Sponsoring Organization (COSO)

Established automated payment systems

- Both significant online presence (stored credit cards) and point-of-sale machines subject to security failures

Adherence to industry standards

- Subject to PCI Security Standards/Plastic Card Security Statutes

Exposure to litigation

- Frequent litigation target following data breach

Privacy and security policies

- Privacy and security questions surrounding loyalty program information

Key factors where retailers can focus:

- Transparency: It is important that retailers are transparent when collecting customer information. Many consumers are already on edge due to past breach activity in the retail space so transparency is extremely important for consumer confidence
- Comprehensive patching policy: An established patching policy is key to help avoid vulnerabilities, such as those that led to the WannaCry and NotPetya malware attacks
- Ongoing training: Employee training and awareness is still at the core of cyber resilience. As noted in the Global Cyber Risk Transfer Comparison Report conducted by the Ponemon Institute and sponsored by Aon, 34 percent of cyber incidents are due to human error, mistakes and negligence
- Ongoing testing: Having a cyber incident response plan is key but testing regularly is critical. Making sure this plan is up to date and compliant will help greatly in limiting future damage

All descriptions, summaries or highlights of coverage are for general informational purposes only and do not amend, alter or modify the actual terms or conditions of any insurance policy. Coverage is governed only by the terms and conditions of the relevant policy.

Scenario 1: Specialty Retailer Suffers Breach of Customer Credit Card Information

Transfer

Existing Comprehensive Coverage in Place Through Aon

A cyber program with $50M in limits

- Broad form language inclusive of first and third party coverages with limit adequacy determined through peer benchmarking and quantification analysis
- Coverage terms are reviewed on an ongoing basis with changes made as needed
- Self-insured options and retention analysis is identified through robust analytics

Improve

Proactive Incident Response Strategy is in Place

As a best practice, an incident response retainer is in place with Aon Cyber Solutions Group

- We assisted in the development of the Incident Response Plan
- Annual testing and plan updates are facilitated
- Aon support, annual awareness and best practice security training are monitored

System was breached at the store level resulting in thousands of customer credit records being released

Retailer immediately notifies Aon

Desired Outcome

Situation is addressed as follows:

Improve

Respond

First Party Costs Incurred Post-Breach

- Forensics experts determine what information is compromised and whether or not the “bad actor” is still in their system
- Notification experts alert those whose information was compromised
- Credit monitoring is provided for affected individuals
- Public Relations is notified to restore trust with consumer base
- Legal expenses to remain compliant post-breach

Third Party Liability Incurred Post-Breach

- Defense costs against a third party class action bringing suit for having their information breached
- Settlement with stakeholders including banks and credit unions, credit card issuers, consumers and various U.S. states

Claims Advocacy and Forensics

The Aon Claims Advocacy team notifies the cyber insurance carriers

Using the Incident Response Plan, the retailer works with the Legal and Forensics team from Aon to:

- Maintain and control information in response to breach
- Interact with regulatory officials
- Remediate the damage and help restore normal business operations
- Provide support to notify and protect customers

The Aon Claims Advocacy team helps protect the balance sheet by developing and presenting the cyber claim

- Captures the information necessary to measure impact and loss
- Coordinates and supervises insurance adjuster inquiries and inspections
- Advises on coverage and negotiates with insurer(s)
- Recognizes and engages with other lines of coverage for maximum recovery
- Facilitates continuity and delivery of coverage

Scenario 2: Retailer's Concern about Denial-of-Service Attacks

To help the retailer improve their Risk and IT teams' response to a potential denial-of-service attack, they are interested in the following:

- Quantifying the negative financial implications that may arise from a cyber-related event that results in a significant interruption to their operations
- Quantifying and addressing the loss of revenue that occurs due to an inability to transact business
- Understanding whether they have a robust cyber insurance policy to respond to situations like denial-of-service
- A comprehensive approach to assess vulnerabilities, security governance operations, controls to improve and measure cybersecurity posture, aligned with proven security frameworks

Assess

Aon Cyber Diagnostic Tool

The retailer completes the free Aon Cyber Diagnostic Tool, an online survey to provide high level guidance on the organization's preparedness for cyber attacks

Result: the retailer enlists Aon to review

- A cyber security risk assessment is conducted capturing material risk exposures to critical technology assets
- A control performance assessment of security posture is conducted in order to identify plausible cyber threat scenarios for risk quanitification and risk transfer decision making

Desired Outcome

Situation is addressed as follows:

Quantify the Financial Impact

Quantify

To address the specific loss quantification needs of the retailer, the Aon Data and Analytics team conducts a sophisticated analysis (including all perils and risk scenarios) to evaluate potential self-insurance options

- The analysis offers the retailer a loss quantification of its cyber exposure in terms of worst case estimated maximum loss (EML) and probable maximum loss (PML), considering both first and third party exposures
- The retailer is empowered to make an informed decision on structuring its cyber insurance tower by maximizing its risk financing and self-insurance needs through the utilization of its captive insurance company
  - Cyber Extortion and Business Interruption coverages are included in the risk transfer program to address internal and external threats

Optimize and Uncover Risk

Test

Improve

To achieve a higher level of cyber resilience, the testing services provided by Aon Cyber Solutions Group are conducted to enhance the security posture of the retailer

- The risk factors specific to the retail industry are assessed relative to likely attack vectors and existing security controls to produce prioritized remediation recommendations
  - The Aon team tests and identifies potential application, network and endpoint risks utilizing the tools, tactics and procedures employed by the retailer's adversaries
- An effective security posture requires constant validation, measurement and improvement. The Aon team helps the retailer to develop and adopt strong security governance programs and policies to improve overall security architecture and design, enabling it to be in compliance with industry standards and operate with confidence

Contacts

MaryAnne Burke
Retail Industry Practice Leader
Aon
+1.203.326.3463
maryanne.burke@aon.com

Julie Layton
Deputy Retail Industry Practice Leader
Aon
+1.305.961.6214
julie.layton@aon.com

James Burnett
Assistant Vice President
Financial Services Group
Aon
+1.952.807.0892
james.burnett@aon.com

Rocco Grillo
Cyber Consulting Leader
Aon Cyber Solutions Group
+1.212.981.2674
rocco.grillo@aon.com

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

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

GDM069460081018

Empower Results®