# 2018 MANAGED SECURITY SERVICE PROVIDER (MSSP): BENCHMARK SURVEY

Insights That Inform Decision-Making for Retail Industry Outsourcing

R-CISC
THE RETAIL ISAC

*Powered by the Retail ISAC, A Division of the R-CISC*

## Overview

Last October, the Retail Cyber Intelligence Sharing Center (R-CISC) released its first Strategic Benchmark Report produced in partnership with Retail Industry Leaders Association (RILA) followed by a related workshop led in partnership with Deloitte at the 2017 Retail Cyber Intelligence Summit. During the workshop, chief information security officers (CISOs) from more than 10 retail companies provided input that informed the next phase of benchmarking projects.

The group elected to form the CISO Steering Group, with participating CISOs including Rich Agostino from Target, Lauren Dana Rosenblatt from The Estée Lauder Companies, and Dave Spooner from the TJX Companies providing expertise on R-CISC benchmarking programs to address the growing challenge for CISOs from retail to provide strategic metrics that articulate the impact of security investments on business revenue. By harnessing input from member contributors and insight from industry partners, the group's goal is to produce a series of focused surveys that inform member-derived products built to improve visibility, decision-making and prioritization abilities for CISOs.

The first in this series of surveys was the Managed Security Service Provider (MSSP) Benchmark Survey. The R-CISC consulted Deloitte for expertise to develop the MSSP Survey of its members, which included approximately 22 multiple choice questions. Forty-five companies encompassing the following industries participated: retail, restaurants, hotels, gaming properties and consumer packaged goods.

*"For CISOs and their teams, benchmarking metrics and information sharing with retail industry peers provides visibility and useful context to build confidence from a strategic perspective and situational awareness at a tactical level. Whether our focus is on strategic planning or assessing our cyber threat programs, sharing information is a critical step that can help influence how we evolve our abilities to better protect our consumers, employees and brands."*

Lauren Dana Rosenblatt
Deputy Chief Information Security Officer (CISO)
The Estée Lauder Companies

*"While retail and hospitality businesses may have similar transaction volumes as some of their banking counterparts, they typically have smaller information security teams and spend. We observe that CISOs from our retail clients are finding ways to do more with less, helping their organizations secure tomorrow's growth in a world of shifting consumer expectations."*

Upen Sachdev
Principal
Deloitte & Touche LLP

## Goals

The MSSP Benchmarking Survey findings articulate retailer budgeting considerations related to MSSPs, including: MSSP usage patterns, MSSP selection process and budget observations, MSSP outsourcing experiences, and expectations on future spend that frame the scope for retailer outsourcing and inform MSSP decision making capabilities.

The full 2018 Managed Security Service Provider (MSSP) Benchmark Survey report is available to R-CISC Core members. The R-CISC has compiled this summary as a resource for meaningful insight that benefits the broader retail industry ecosystem, partners in government, and the cybersecurity community at-large.

## Key Findings

Survey results illuminated use and experience of how retail and consumer-facing industries leverage MSSPs. Respondent companies span the retail channels and include: retail, restaurants, hotels, gaming properties, consumer financial services and consumer packaged goods. Key findings are broken down into four categories: MSSP Usage Patterns, MSSP Selection Process, Outsourcing Experience and Expectations on Future Spend.

## Quality of Service/Service Level Agreements

Next generation CISOs are leading in-house innovation while relying heavily on managed security service providers for other services. Interestingly, **Innovation by the MSSP** and **MSSP Ratings** reported by top global research and advisory firms have the least amount of influence on MSSP selection. **Quality of Service/Service Level Agreements** (SLAs) have weighed in as the most important MSSP decision-making factor, with Price/Value following closely behind.

## Talent and Budget Constraints

**Talent and budget constraints** remain top problems. A whopping **92%** of respondents report that the cost of developing and maintaining in-house talent, and/or challenges attracting and retaining talent are top reasons for leveraging MSSP services. Related, **42%** experience challenges **attracting and retaining talent**, making this a **key factor** in the decision to leverage MSSP services.

## Event Monitoring

**90%** of respondents are leaning on managed security service providers to provide **event monitoring** for IT infrastructure logs, **firewalls** and **intrusion detection systems** (IDS)/**intrusion prevention systems** (IPS). Interest in **threat intelligence** and **dark web monitoring** services is growing - **23%** of respondents will likely leverage these MSSP services in 2019.

## Maximizing Efficiencies

Projected MSSP spend reflects the need for CISOs to maximize efficiencies while driving a year-over-year investment mentality - **15% of respondents foresee their MSSP spend going down**; however, **36% indicate that they are likely to increase their MSSP spend**.

## Conclusion

Organizations of different sizes show differing appetites for subscribing to and leveraging MSSP services. Due to increasing cost concerns and challenges faced with in-house talent, participating organizations are looking to outsource the security functions to an MSSP instead of building the capability in house for monitoring events from IT infrastructure logs, firewalls, and IDS/IPS, as well as to conduct penetration tests. Many participating organizations indicate that they're likely to increase spend or retain 2018 budgetary spend for MSSPs in the coming year. Organizations cannot remain static—the risks evolve, and so organizations must adopt a year-over-year investment mentality.

## About R-CISC

The R-CISC is the trusted cybersecurity community for retailers, consumer products, grocers, hotels, gaming, restaurants, consumer financial services and cybersecurity industry partners worldwide. The R-CISC supports its member base, representing more than $1 trillion in annual revenue, by serving as the conduit for collaboration, cooperation, and threat and best-practice sharing. Through building and sustaining valuable programs, partnerships, products and opportunities, the R-CISC enables its members to deepen their trust-based relationships, strategic knowledge and tactical capabilities. For more information on the R-CISC and how to join, visit r-cisc.org. Connect with us on Twitter and LinkedIn.

*"All companies, including retailers, need to constantly adapt to stay ahead of today's cyber threats. Benchmarking with other companies plays an important role in enhancing our security program at Target, supporting our team's continuous improvement and getting visibility into the state of the industry. Cyber security shouldn't be considered a competitive advantage, but a collaborative effort. Each company's willingness to actively share information is crucial; the more we share, the better we become at defending our companies and strengthening the capabilities of the retail industry."*

Rich Agostino
CISO
Target Corporation