# R-CISC

## THE RETAIL ISAC

# 2018 Annual Report

# R-CISC
### THE RETAIL ISAC

## TABLE OF CONTENTS

As one of the founding members of R-CISC, I joined because I believed in the mission and still do. We as an industry needed to come together and join forces to collaborate on our common cybersecurity risks. I believe strongly in the quote, "A rising tide lifts all ships." If we as the R-CISC community can help one another, then the entire industry will be stronger.

Colin Anderson
Global CISO
Levi Strauss & Co.

Chair, R-CISC Board of Directors

## INTRODUCTION

R-CISC members deliver shopping, hospitality, dining, entertainment, and gaming services and experiences for customers around the globe. We recognize that cyber threats are a strategic business risk and that as retail and customer-facing companies, we are better able to protect our customers and our brands when we work collectively to address cyber threats.

## VISION

To reduce cyber risks to retail and consumer-facing sectors.

## MISSION

We enable retail and consumer-facing sectors to mitigate cyber risk by establishing trust, expanding knowledge and maturing capability through information and intelligence sharing.

## Membership by the Numbers

### Growth Milestones Since Founded

**2018 YEAR END** — 136 Members

**2017 YEAR END** — 107 Members

**2016 YEAR END** — 83 Members

**2015 YEAR END** — 45 Members

**136** Member Companies

**945** Practitioner Analysts, Managers, Directors, and CISOs

**700+** Retail and Hospitality Brands

## Members are Talking

"Excellent source for learning about new/developing threats in retail industry. Very good sounding board for questions related to retail security issues and offers good opportunity to network with peers."

"Extremely helpful to have a forum to build new trusted peer relationships and be able to compare notes with like companies. This accelerates problem solving and makes my company more resilient."

"Day to day knowledge/intel sharing for my analysts and conversations around franchises and other best practices are always very beneficial."

## Protect as One
### About the R-CISC

The R-CISC was formed in 2014 as the home of the Retail Information Security and Analysis Center (ISAC) and operates as a central hub for sharing sector-specific cyber security information and intelligence. The association connects information security teams at the strategic, operational and tactical levels to work together on issues and challenges, to share practices and insights, and to benchmark among each other – all with the goal of building better security for the retail and hospitality industries through collaboration. R-CISC currently serves companies in the retail, hospitality, gaming, travel and other consumer-facing entities.

Through the Cyber Information Sharing and Collaboration Program (CISCP), the R-CISC participates in sharing of threat information throughout the agencies affiliated with DHS, including the Federal Bureau of Investigations, U.S. Secret Service, and organizations such as the United States Computer Emergency Readiness Team (US-CERT) and others affiliated with the National Cybersecurity & Communications Integration Center (NCCIC). The R-CISC is also a member of the National Council of ISACs (NCI), enabling the R-CISC to share critical cross-industry threat and vulnerability information and requests for information, to gain insights and collaborate on cybersecurity issues, physical threats and coordination during national-level events.

# BOARD OF DIRECTORS

## OFFICERS

### CHAIR
Colin Anderson, Global CISO
Levi Strauss & Co.

### VICE CHAIR
Scott Howitt, SVP & CISO
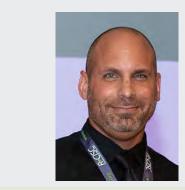MGM Resorts International

### TREASURER
Dave Spooner, SVP & CISO
Staples, Inc.

### SECRETARY
Grant Sewell, Manager, Global Information Security
Scotts Miracle-Gro Company

### PRESIDENT
Suzie Squier, President
R-CISC

## DIRECTORS

Jim Cameli, VP & Global CISO
Walgreens Boots Alliance
Past Chair, R-CISC

Ken Athanasiou, CISO
AutoNation, Inc.

Lauren Dana Rosenblatt, Deputy CISO
The Estée Lauder Companies, Inc.

Warren Steytler, CISO & VP IT, Engineering & Operations
Lowe's Companies, Inc.



The R-CISC provides the ideal platform for focused, peer-to-peer sharing and thought leadership central to what lies ahead as we work to solve our toughest industry problems together. From daily threat intel and best practice sharing to participating on the steering committee for the franchised business group, I'm proud of the energy and the commitment that we have as a community to collaborate and collectively address cyber risks.

Christopher Zell, Senior Director, Head of IT Security
Wendy's Company

## TOP TRENDING

### WEBINARS

Top Five Retail Payment Threats

Presented by:
Glen Jones, Head of Payment Systems Cyber Intelligence
Visa Threat Intelligence

Behavioral Authentication -
The Next Generation of Identity and Access Validation

Presented by:
Jim Routh, CISO
Aetna
*and*
Brett McDowell, Executive Director
FIDO Alliance

New Attack Trends in Retail

Presented by:
Mengmeng Chen, Retail Threat Intelligence Lead
Shape Security

Intelligence shared through the R-CISC has played a key role in our efforts to combat cyber threats. We can directly correlate the value gained in the form of actionable intelligence, boosting our overall capability to better protect our organization and the community as a whole.

**Rick Rampolla**, Senior Manager, IT Security
Publix Super Markets, Inc.

## Intelligence + Best Practice
## Information Shared

**Webinars**
33 in 2018; 629 total participants

**Intelligence Workshops**
114 cybersecurity professionals participated across 5 workshops, hosted by Deloitte, Publix Supermarkets, Inc., Sally Beauty and Target

**Dedicated Task Force, Working Group, + Committee Groups**
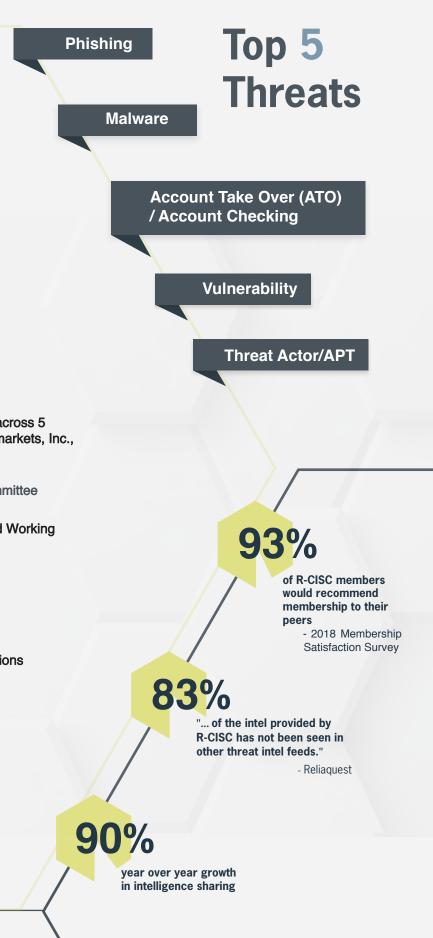10 Member-led Committees, Task Forces and Working Groups

**Retail Cyber Intelligence Summit**
220 total participants

**Collaboration Portal**
719 documents shared; 293 member discussions

## Top 5 Threats

Phishing

Malware

Account Take Over (ATO) / Account Checking

Vulnerability

Threat Actor/APT

**93%**
of R-CISC members would recommend membership to their peers
- 2018 Membership Satisfaction Survey

**83%**
"... of the intel provided by R-CISC has not been seen in other threat intel feeds."
- Reliaquest

**90%**
year over year growth in intelligence sharing

## Member Satisfaction
by the numbers

## 2018 HIGHLIGHTS

### APRIL
**2018**

R-CISC announces formation of Gaming and Hospitality Cybersecurity Alliance

### MAY
**2018**

Fraud Committee releases Best Practices for Mitigating Coupon Fraud

### JUNE
**2018**

R-CISC releases Growth of Business Email Compromise in the Retail Sector

### JUNE
**2018**

R-CISC demonstrates commitment to building awareness and providing support for Retailers in Canada with its inaugural Toronto Intelligence Workshop

### JULY
**2018**

R-CISC announces Advisory Council of leading trade associations representing merchant industries

### AUGUST
**2018**

CISO Committee releases 2018 Managed Security Service Provider (MSSP) Benchmark Report: Insights that Inform Decision-Making for Retail Industry Outsourcing

### OCTOBER
**2018**

R-CISC launches curated Intelligence Analysis Report for member analysts and other technical subject matter experts

### OCTOBER
**2018**

R-CISC holds its third annual Retail Cyber Intelligence Summit and announces Peer Choice Award Winners

### NOVEMBER
**2018**

R-CISC launches Executive Intelligence Report for senior cybersecurity strategists

# Member-Led + Member Driven
## FOCUS GROUPS



Gaming and Hospitality Cybersecurity Alliance members offer a vast array of services and experiences in entertainment, gaming, sporting events, dining, shopping and hospitality. Recognizing we are stronger acting against bad actors together, our goal is to build trust and share information and actionable intelligence which will strengthen not only each company, but our industries.

**Scott Howitt**
SVP & CISO
MGM Resorts International

Vice-Chair
R-CISC Board of Directors

## CISO Committee

**Committee Chairs**
Rich Agostino, CISO
Target

Cory Mazzola
Executive Director, Global Cybersecurity Operations
Las Vegas Sands Corporation

Lauren Dana Rosenblatt, Deputy CISO
The Estée Lauder Companies

George Smirnoff, CISO
Synchrony

Dave Spooner, SVP & CISO
Staples, Inc.

## Gaming & Hospitality Cybersecurity Alliance (GHCA)

**Alliance Chairs**

Steve Begalman, VP, Information Security
Boyd Gaming

Scott Howitt, SVP & CISO
MGM Resorts International

Cory Mazzola
Executive Director, Global Cybersecurity Operations
Las Vegas Sands Corporation

## Securing Retail Alliance (SRA)

**Alliance Chairs**
Tim Crothers, VP, Security
Target

Mike Cushing, Network & Security Engineer
Patagonia

## Fraud Committee

**Committee Chairs**
René Lopez, Manager, Threat Intelligence
Amazon.com, Inc.

Ryan Miller, Senior Manager, Cyber Threat Intelligence
Target

Rick Rampolla, Senior Manager, IT Security
Publix Super Markets, Inc.

## ISAC Committee

**Committee Chairs**

Adam Hirsch, Director, Information Security
PVH Corporation

Adam Souza De Almeida, Senior Cybersecurity Analyst
Canadian Tire Corporation Limited

Ken Anthanasiou, CISO
AutoNation, Inc.

Colin Connor, Director, Threat Intelligence & Cyber Forensics
AT&T

Kia Hakimi, VP, Global Threat Detection & Response
Best Buy

Lauren Dana Rosenblatt, Deputy CISO
The Estée Lauder Companies, Inc.

## Franchise Committee

**Committee Chairs**

Lara Divi, VP & CISO
Dine Brands Global

Sailaja Kotra-Turner, Senior Director, IT Security & Risk Management
Brinker International

Christopher Zell, Senior Director, Head of IT Security
Wendy's Company

Signe Jackson, Principal, Retail Technology Security
AT&T

## Content Oversight Committee

**Committee Chairs**
Lauren Dana Rosenblatt, Deputy CISO
The Estée Lauder Companies, Inc.

Grant Sewell, Manager, Global Information Security
Scotts Miracle-Gro Company

William Hahn, CTI Analyst
TJX Companies

## Engagement Oversight Committee

**Committee Chairs**
Vijay Bolina, CISO
Blackhawk Network

Roseann Larson, Former CISO
VF Corporation

George Smirnoff, CISO
Synchrony

Dave Spooner, SVP & CISO
Staples, Inc.

# Top Trending Content

## Fin7 Cyber Threat Hunt Cards
by Gap Cyber Defense Center

Published March 2018 | 102 views

Receiving 102 member views, this document applies the Cyber Threat Hunt Card methodology to characterize the FIN7 threat and report on the identified Indicators of Compromise (IOC) to support a hunt hypothesis and identify the hunt direction. From the Gap CDC team: "The overall goal is to empower cyber threat hunters to understand how the adversary moves throughout the Cyber Kill Chain and use that knowledge to boost detection."

## TLP: Red Retailer Investigates Active Advanced Persistent Threat Incident

Published August 2018 | 157 views

In August 2018, a member retailer reported details of an active threat incident investigation of an advanced persistent threat on their network. The retailer provided information including suspected actor motivation based on the potential targets, activity on the impacted services/devices, and the fact that the TTPs utilized were very similar to those seen in two recent breaches that had not been disclosed to the public.

Over 150 R-CISC members accessed the related intelligence report, leveraging the associated indicators and related context to proactively hunt for threat indicators, improve defense, and effectively reduce the risk of their own companies being impacted by the same attack.

Intelligence is useless if you're operating in a vacuum. The true value of the R-CISC is that it brings together retail cyber intelligence professionals from across industry and provides a forum for us to share information and ideas. Within the R-CISC community, my peers and I rely on one another for help with putting pieces of the puzzle in place, which is not only rewarding, but also a great weapon in the fight to help secure my organization.
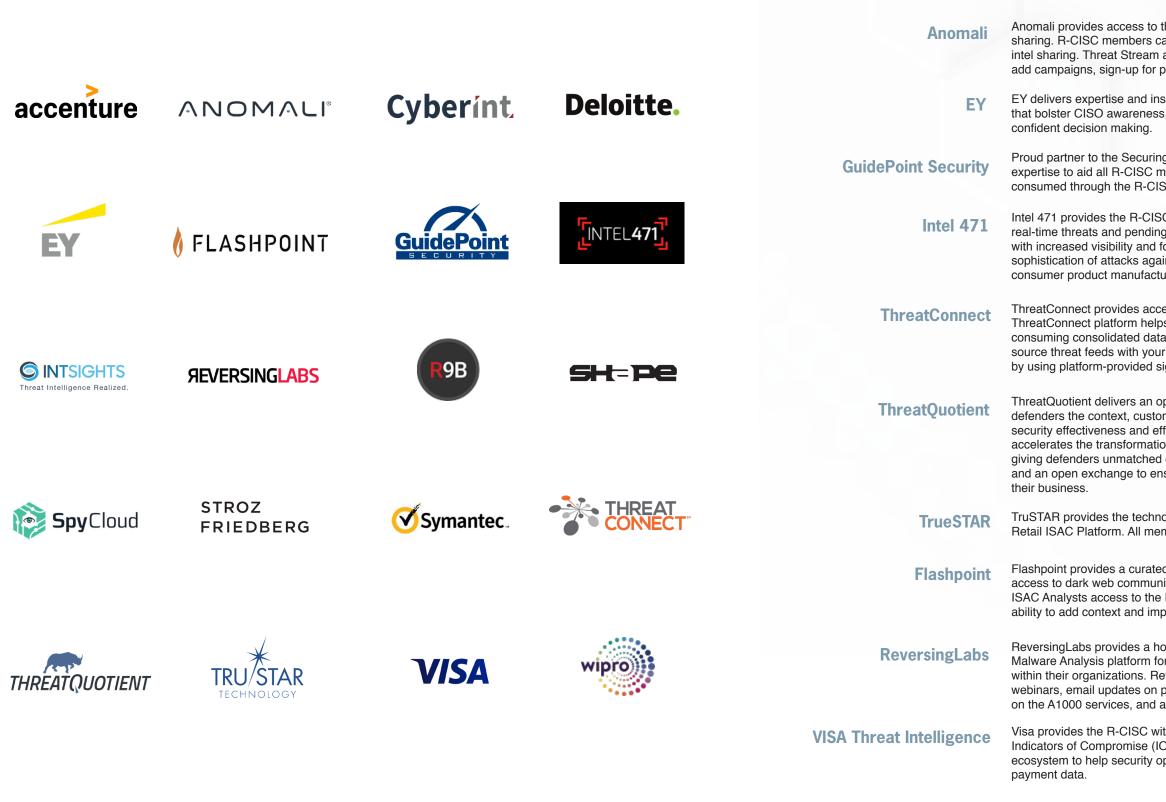
**Jason Lay**, Threat Intelligence Lead, Qurate Retail Group

## PEER CHOICE
## AWARD WINNERS

CISO OF THE YEAR
**Rich Agostino**
CISO, Target

CYBERSECURITY TEAM OF THE YEAR
**Information Security Team**
Target

BREAKTHROUGH FEMALE IN CYBERSECURITY
**Angeline Button**
Lead, Threat Hunting and Intelligence
Dillard's

**Vanessa Aranda**
Threat Intelligence Analyst
Gap, Inc.

CYBERSECURITY PRACTITIONER OF THE YEAR
**Ryan Miller**
Senior Manager, Cyber Threat Intelligence
Target

ASSOCIATE MEMBER OF THE YEAR
**Intel 471**

FAST STARTER AWARD
**Wendy's Company**

**Anomali** — Anomali provides access to their Anomali Threat Stream portal site for R-CISC intel sharing. R-CISC members can create their user accounts and join trusted circles for intel sharing. Threat Stream account holders can then view incidents, add incidents, add campaigns, sign-up for phishing email ingest and import indicators.

**EY** — EY delivers expertise and insight for curated R-CISC Executive Intelligence reports that bolster CISO awareness, improve visibility of retail industry threats and support confident decision making.

**GuidePoint Security** — Proud partner to the Securing Retail Alliance, providing relevant content and expertise to aid all R-CISC members in maximizing the value of threat intelligence consumed through the R-CISC, along with savings for members.

**Intel 471** — Intel 471 provides the R-CISC ISAC team with timely and exclusive data on current, real-time threats and pending future threats. This partnership provides the R-CISC with increased visibility and focused insight related to the increased number and sophistication of attacks against retailers, online commerce, restaurants, hotels, consumer product manufacturers and other consumer serving industries.

**ThreatConnect** — ThreatConnect provides access to their platform for R-CISC members. The ThreatConnect platform helps to identify, manage and block threats faster by consuming consolidated data, importing your own data, combining external open source threat feeds with your data, and allowing you to act on malicious indicators by using platform-provided signatures to detect threats in your environment.

**ThreatQuotient** — ThreatQuotient delivers an open and extensible platform to provide R-CISC defenders the context, customization and collaboration needed for increased security effectiveness and efficient threat operations and management. ThreatQ accelerates the transformation of threat data into actionable threat intelligence by giving defenders unmatched control through a threat library, an adaptive workbench and an open exchange to ensure that intelligence is accurate, relevant and timely to their business.

**TrueSTAR** — TruSTAR provides the technology infrastructure that forms the backbone of the Retail ISAC Platform. All members receive up to 5 complimentary user logins.

**Flashpoint** — Flashpoint provides a curated intelligence report for members, in addition to granting access to dark web communities for greater visibility of threats, and grants the Retail ISAC Analysts access to the Flashpoint intelligence portal, aiding the R-CISC's ability to add context and improve overall insight on threats.

**ReversingLabs** — ReversingLabs provides a hosted and maintained online instance of the A1000 Malware Analysis platform for all R-CISC members to share threat information within their organizations. ReversingLabs offers training for users including quarterly webinars, email updates on product offerings and benefits, in-depth presentations on the A1000 services, and availability for direct user support.

**VISA Threat Intelligence** — Visa provides the R-CISC with threat briefings and a library of breach-validated Indicators of Compromise (IOCs) from attacks against all sectors of the payments ecosystem to help security operations detect and protect against attacks targeting payment data.

**Deloitte** — Deloitte partners strategically with the R-CISC to provide consultative expertise and research for the CISO Group's strategic benchmarking program. Nearly $100K in expertise contributed to CISO benchmarking research.

**For membership information, please contact membership@r-cisc.org**