R-CISC RETAIL CYBER INTELLIGENCE SHARING CENTER

Membership Guide

R-CISC GREEN

April 2015

Table of Contents

R-CISC RETAIL CYBER INTELLIGENCE SHARING CENTER

Dear Member:

I want to personally welcome you to the Retail Cyber Intelligence Sharing Center (R-CISC). We are excited by the opportunity to work together with you within the trusted community of fellow retail and consumer services security professionals.

Our work in information sharing has never been more important than it is today. Our adversaries share information on how to attack our organizations individually as well as the industry as a whole. Our ever-expanding community shares information on how to defend against these attacks, protect valuable resources, and earn the trust of our customers. We have been able to draw upon the desire of our members and partners to protect their companies and the commercial infrastructure of the country. It is this collective determination of the community enabled by the R-CISC that we strive to deter our adversaries' greed and desire to do harm.

In a very short time we have seen the R-CISC grow from inception to reality, and with the support of the growing member community we continue to see great success achieved through sharing. Looking forward, I am greatly encouraged by the amount of enthusiasm from our members and partners, and by the support of our government. We will continue to expand our use of threat intelligence and refine the application of it through the application of the research, education, and training elements of the R-CISC.

We have created this guide as a means to ensure you're taking advantage of all of the products and services your membership has to offer. We hope it will provide you with valuable information on how to get started. Please direct any questions about its content to membership@r-cisc.org.

Sincerely,

Brian A. Engle
Executive Director
Ph. (202) 679-5670
@brianaengle
www.r-cisc.org

R-CISC RETAIL CYBER INTELLIGENCE SHARING CENTER

1. What is the R-CISC

The Retail Cyber Intelligence Sharing Center (R-CISC) is the primary cybersecurity resource for the retail and commercial services industries providing a critical tool in the arsenal against cyber-attacks. Through the R-CISC, members of all sizes share cyber intelligence on incidents, threats, vulnerabilities, and associated threat remediation. We're stronger through collaboration.

The R-CISC was unveiled in May 2014, and in June, many major retailers began sharing threat intelligence among themselves with analyst support and with feeds from the NCCIC, FBI and other government sources. Developed with the input of more than 50 retailers, the R-CISC consists of three key components:

R-CISC Information Sharing & Analysis Center (ISAC): brings retailers together for omni-directional sharing of actionable cyber threat intelligence, and functions as a conduit for retailers to receive threat information from government entities and other cyber intelligence sources.

Education & Training: works with retailers and partners to develop and provide both education and training to empower information security professionals in retail and related industries.

Research: looks to the future, undertaking research and development projects in partnership with academia, thought leaders, and subject matter experts in order to better understand threats on the horizon.

Together, these components will help retail and commercial services companies enhance their capabilities to protect their enterprise and their customers.

1.1 Membership

The R-CISC includes firms engaged in the operation of a retail presence that are connected with the retail merchandising industry (e.g., wholesalers or product manufacturers), restaurant or food service industry, sports leagues (e.g., professional sports leagues and federations), gaming (e.g., casinos), lodging (e.g., hotels, motels, conference centers), outdoor events (e.g., theme and amusement parks, fairs, campgrounds), entertainment and media (e.g., motion picture studios, broadcast media) or other commercial services, whether physical or internet-based.

Membership in R-CISC is open to retailers, merchants and commercial services organizations of all segments and sizes.* Due to the nature of the retail industry, the R-CISC Board ensured that membership dues would allow retailers of all sized to reap the benefits brought by the power of the retail industry. The R-CISC is currently endorsed by the Retail Industry Leaders

Association (RILA), the National Retail Federation (NRF) and the American Apparel & Footwear Association (AAFA).

*Subject to R-CISC approval.

1.2 Participation

To ensure maximum membership benefit and information sharing, we highly recommend representatives from the following roles within organizations obtain access to the R-CISC's resources:

- CISO
- Head of IT Risk
- Security Operations
- IT Operations
- Threat Intelligence
- Physical Security
- Incident Response
- Business Continuity
- Disaster Recovery
- Fraud Investigations
- Audit/Compliance
- Payments
- Risk Management

2. R-CISC Governance

The R-CISC is a non-profit organization established to provide support and services to its members. All strategies, projects, products, and services are driven by member feedback.

2.1 R-CISC Information Sharing & Analysis Center (ISAC)

The R-CISC ISAC monitors member submissions, open source websites, government intelligence, and private sources of information for real-time cyber threat, vulnerability, and attack intelligence which is quickly disseminated and shared in the form of alerts to members. This real-time analysis and information sharing flow enables members' ability to mitigate the risk of cyber-attacks on their organization and customers.

3. Membership Benefits Currently Available

The R-CISC utilizes information sharing, education and research to aid the industry with situational awareness regarding new cyber security threats, incidents, and challenges. The forefront benefit of R-CISC membership is the real-time member-to-member information sharing that enables all participants to improve their cybersecurity posture, respond to attacks and emerging threats, and strategically address risks individually and collectively.

Upon joining the R-CISC, new members can immediately consume intelligence and become active participants in sharing outwardly with their peers within the community. To enable new members to engage immediately within the secure information sharing portal, a recorded version of the R-CISC new member portal training is available to be viewed on-demand in the Documents tab of the portal under Member Resources.

3.1 R-CISC ISAC Portal

The R-CISC ISAC's portal serves as the primary mechanism to share and disseminate relevant, timely, and actionable alerts associated with cyber incidents, threats, vulnerabilities, and solutions associated with the retail sector's critical infrastructures and technologies. The information is shared securely via the portal among members of the R-CISC using two-factor authentication, and can occur both anonymously as well as openly. Portal access is provided upon initiation of R-CISC membership.

An organization's primary point of contact coordinates the distribution of portal users' IDs and two-factor authentication tokens. **All new user or change requests for portal access must be requested through the primary point of contact**.

Any technical issues with portal access should be directed to 1-877-624-3771 or Portal.Helpdesk@r-cisc.org. Please update your email white lists to include this address to ensure proper delivery of all portal alerts: undeliverable@r-cisc.org.

3.1.1 Member Submission

Member submissions are the primary means for sharing information across the membership. Organizations can choose to share information on the secure portal with attribution or anonymously.

3.1.1.1 Traffic Light Protocol (TLP)

The R-CISC follows strict information handling procedures using the Traffic Light Protocol (TLP). All information submitted, processed, stored, archived, or disposed of is classified and handled in accordance with the following classification. Unless otherwise specified, all information is treated as confidential information (Amber) and is not disclosed to parties outside of the R-CISC without the permission of the originator. Information must be disclosed, transported, stored, transmitted, and disposed of in a safe and secure manner using controls appropriate to the level of classification. These controls include, but are not limited to, encryption, shredding, securely erasing, and degaussing of media. The table below describes the classifications of information and intended audiences.

Color	When should it be used?	How may it be shared?
RED	Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
AMBER	Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
GREEN	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or

	peers within the broader community or sector.	community, but not via publicly accessible channels.
WHITE	Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

3.1.1.2 Submission Process

Members log into the portal using a two-factor authentication token in order to submit data either anonymously or with attribution. Analysts will categorize member submissions into appropriate alert types, utilize various analysis tools and resources to further investigate the threat information, and include additional findings.

Analysts will prioritize member submissions by assessing the associated risk, criticality, and urgency which may vary depending on the threat information. Member attribution in member submissions will be sanitized for anonymous member submissions at all times unless the originator requests otherwise.

Alerts will be disseminated to appropriate audiences in a timely manner and continuously updated as additional intelligence is being collected.

For questions about submitting alerts or the content of alerts, contact the R-CISC ISAC at isac@r-cisc.org, or 571-366-4509, prompt 2.

3.1.2 Additional Portal Features

Aside from housing the member submissions module, the portal contains a number of additional information resources readily available for member consumption.

3.1.2.1 Intelligence Viewer

View previous portal alerts within the Intelligence Viewer tab. A search feature enables organizations to query by a particular topic of interest.

3.1.2.2 Document Library

A document library allows members to search on particular topics of interest or retrieve documents previously posted to the portal.

3.1.2.3 Membership Directory

The membership directory allows members to reach out directly to various points of contact at an institution if there is a threat that requires immediate action. Organizations have the flexibility to include as many contacts as they deem necessary.

The primary point of contact can view and export the list of users and last login dates from their own organization to assist in managing portal usage. A user guide is located in the portal within the Documents tab in the Portal Training Materials folder.

3.1.2.4 CISCP Information

All members receive cyber threat indicators from government partner DHS CISCP (Cybersecurity Information Sharing and Collaboration Program) upon execution of an agreement with DHS.

3.2 R-CISC ISAC Listserv

The R-CISC ISAC listserv is an attributable, open discussion mailing list that facilitates the discussion of retail and commercial service industry cybersecurity matters within the R-CISC community. It is meant to assist the community participants with sharing information broadly to advance their capabilities to defend against threats and reduce risks. This peer-to-peer information sharing within the community enables members to learn what others are doing tactically to combat threats along with mitigation strategies. The contents of this list are TLP: GREEN, and subscribers of the R-CISC ISAC list may share information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

The R-CISC listserv is open to all R-CISC members. It is highly encouraged for all members to remain subscribed to this mailing list throughout their R-CISC membership to receive timely information related to the retail and commercial services industries as it pertains to threat intelligence and information sharing. Please note that email messages from the R-CISC listserv are not generated by the R-CISC ISAC member portal.

To post to the list, put the list address ISAC-listserv@subscribe.r-cisc.org in the "To:" field of the email. Any posts made to the R-CISC list will go to all subscribers on the list, so please utilize it with discretion. Also, members are advised to properly obfuscate threat indicators (URLs/domains) and zip/password-protect malicious attachments, and are also encouraged to utilize the secure R-CISC member portal for the exchange of specific threat details and information that is considered TLP:RED or TLP:AMBER.

Please direct any questions or support needs related to the R-CISC ISAC-listserv to ISAC@r-cisc.org.

3.3 Machine-Readable Threat Indicator Feed

Core+ members can receive machine-readable threat indicators that can be integrated into systems that support the Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII) capabilities to rapidly detect and respond to threats and attacks. Below is a discussion of the R-CISC ISAC Cyber Intelligence Repository and Soltra Edge application.

3.3.1 R-CISC ISAC Cyber Intelligence Repository

The cyber intelligence repository is an automated mechanism for ingesting threat, vulnerability, and event data into members' internal intelligence analysis systems. Based on industry leading security standards such as STIX and TAXII, the repository disseminates structured and near instantaneous critical security information. A large benefit of this repository is the ability to ingest past indicators into an organization's critical infrastructure upon initial login, or at any one point in time. All members are eligible to gain access to the features of the repository. Email membership@r-cisc.org to gain access to the repository.

3.3.2 Soltra Edge

Soltra is a joint venture between the Financial Services Information Sharing & Analysis Center (FS-ISAC) and DTCC. The first product released by Soltra, called Soltra Edge, is an on-premise software solution designed to take in massive amounts of cyber threat intelligence from a variety of sources, normalize this intelligence using the emerging STIX open standard and route this information using the emerging TAXII open standard, allowing organizations to take immediate action. The R-CISC ISAC Cyber Intelligence Repository, discussed above, is one of the intelligence feeds that flows into the Soltra Edge solution.

The basic version of Soltra Edge, which contains the features most needed by many organizations, is now available for download at no cost at www.soltra.com. For more information, please contact info@soltra.com.

4. Alert Management

The R-CISC is proud to be the number one provider of cyber and physical threat intelligence for the retail industry, however, at times the large volume of information can be overwhelming for members to process. Given this, a number of automated processing and filtering mechanisms have been designed to help members process the information in the inboxes and in their environments alike.

4.1 Portal Alert Customization

The portal contains a feature that allows Core + members to customize the type or content of alerts they would like to receive in either HTML or XML format. The Mission Center Quick Reference Guide lists instructions for how to customize alerts, and is located in the Document Library of the portal under Portal Training Materials.

4.2 Email Filtering

Another option for customizing the type or content of alerts a member would like to receive is through email filtering. An alert subject line nomenclature has been created to facilitate the automated parsing and forwarding of alerts using Microsoft Outlook filtering. Microsoft Outlook filtering instructions are located in the Documents tab of the portal under Portal Training Materials.

5. Getting Started

The R-CISC offers members a broad array of ways to get involved. Below is a helpful guide on where to start to make the most out of your membership from the onset.

- **New Member Portal Training** - a recorded version of the R-CISC new member orientation is available to be viewed on-demand in the Documents tab of the portal under Portal Training Materials.

- **Portal Account Setup** - get portal accounts set up for the many business lines that would benefit throughout the organization. This provides all lines of business immediate access to timely and actionable information on past, present, and future cyber and physical threats. Be sure to engage your global resources to ensure the opportunity to get the most out of your membership. Reach out to your primary point of contact to have an account set up.

- **Alert Management**- explore the various ways to filter which alerts you want to see on a regular basis using the Alert Management section of this document.

- **R-CISC ISAC Listserv**- this peer-to-peer information sharing mailing list facilitates the rapid dissemination of cyber intelligence helping to uncover a specific threat or incident as it unfolds, as well as the opportunity to exchange information related to strategic collaboration. You will not want to miss the valuable information provided on a daily basis via participation in this mailing list. Email membership@r-cisc.org to gain access.