



FOCUS e-newsletter: Feature Article
February 2016

Important Cybersecurity Resources for Credit Unions

March 6 – 12 is [National Consumer Protection Week](#). Among the many government agencies and organizations supporting the campaign are several focused on assisting the financial sector better serve members and customers through cybersecurity risk management.

Maintaining awareness of current and emerging threats is increasingly becoming the cornerstone of effective cybersecurity risk management for businesses.

Credit unions should subscribe to one or more information sharing resources to ensure both systems and staff are current and up to date on shifting tactics and methods threat actors use to compromise your institution's information security and systems.

Rapid response to new types of threats can significantly improve an institution's security posture and more effectively help to protect consumer information. There are many sources you can go to acquire threat information including, open source information like the internet and media, paid threat analysis services, federal agency resources, Information Sharing and Analysis Centers (ISAC). While there are a broad range of options with specific and unique attributes, the ISAC's and specifically the Financial Services Information Sharing and Analysis Center (FS-ISAC) is purpose built to provide broad threat information sharing and response resources for the financial services industry including credit unions. FS-ISAC was established in response to Presidential Decision Directive 63 in 1998, and later reinforced by Homeland Security Presidential Directive 7. FS-ISAC is a non-profit private organization that is designed to facilitate threat information sharing, coordinate and improve protection of the Financial Services Sector of the Nation's critical infrastructure. FS-ISAC is a clearing house of information from federal and open resources as well as thousands of financial institutions and service companies worldwide. Credit union management should consider FS-ISAC as a first stop for information resources.

The chart below provides several federal and federally sponsored resources, in order of relevance to the financial services sector, set up to share cyber information.

Resource	Description
Financial Services Information Sharing and Analysis Center (FS-ISAC)	In collaboration with the U.S. Department of the Treasury and the Financial Services Sector Coordinating Council, the Center's mission is to enhance the ability of the financial services sector to prepare for and respond to cyber and physical threats, vulnerabilities and incidents, and facilitate communications during an emergency.

[U.S. Computer Emergency Readiness Team \(US-CERT\)](#)

A resource of the Department of Homeland Security, the Readiness Team leads efforts to improve the nation's cybersecurity, coordinate cyber information sharing and proactively manage cyber risks.

[InfraGard](#)

A partnership between the Federal Bureau of Investigation and the private sector, InfraGard is an association of representatives from businesses, academic institutions, state and local law enforcement agencies and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S.

[Internet Crime Complaint Center](#)

The Center's mission is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners.

[Cyber Information Sharing and Collaboration Program \(CISCP\)](#)

This is the Department of Homeland Security's flagship program for public-private information sharing and complements the Department's ongoing information sharing efforts. Through CISCP, the Department and participating companies share information about cyber threats, incidents and vulnerabilities.