700 SW Jackson Street
Suite 803
Topeka, KS 66603

Kansas
Department of Credit Unions

Phone: (785) 296-3021
Fax: (785) 296-6830
kdcu.office@ks.gov
www.kdcu.ks.gov

Jerel Wright, Administrator

Laura Kelly, Governor

DATE: **May 6, 2019**

BULLETIN: **2019-KDCU-CUB-1**

TO: **Kansas Chartered Credit Unions**

SUBJECT: **Automated Cybersecurity Enhancement Tool (ACET)**

CYBERSECURITY ASSESSMENTS ARE HERE TO STAY… ARE YOU READY?

$5,520,000,000. According to the Internet Crime Complaint Center (IC3), that is the amount of reported loss due to cybercrime between 2013 and 2017. On average, the IC3 receives 800 complaints per day. In 2016, the Financial Crimes Enforcement Network (FinCEN) issued an advisory to financial institutions warning them of being targeted by cybercriminals.

But it might not be criminals that break down the doors to your network. It could be a hardware or software glitch that opens the door for a member (or non-member) to discover a treasure trove of member account information.

Keeping the above in mind, the National Credit Union Administration (NCUA) developed the Automated Cybersecurity Examination Tool (ACET). The ACET mirrors the FFIEC's (Federal Financial Institutions Examination Council) Cybersecurity Assessment Tool, which was developed for voluntary use by credit unions, and consists of two parts: the Inherent Risk Profile and the Cybersecurity Maturity level. Over the next few years, NCUA will be using the ACET to develop a benchmark of the industry's preparedness and determine what improvements need to be made in the credit union system.

Do you have risk management and training in place? Threat intelligence and monitoring? Preventative controls? Incident management and resilience? The related exam worksheet covers areas from anti-virus software to business continuity to penetration tests to physical security. There are many pieces to the cybersecurity puzzle and five domains to the ACET: Cyber-Risk Management & Oversight, Threat Intelligence & Collaboration, Cybersecurity Controls, External Dependency Management and Cyber-Incident Management and Resilience.

The FFIEC recommends an enterprise-wide approach to manage cyber risks with a strong cybersecurity culture as its foundation. This includes implementing preventative controls to minimize the impact and likelihood of a successful attack or breach. If you work with third parties, establish rigorous vender management controls and evaluate their incident response and resilience. Develop policies and procedures to implement your programs.

While either cybersecurity assessment tool may appear overwhelming, it is highly recommended that you commence the process. Now is the time to get a head start on your next exam. Cybersecurity has been an exam priority for many years and the implementation of the ACET reinforces that focus.

NCUA has additional information on the ACET and the FFIEC has resources available on its Cybersecurity Awareness page.