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

Vickie Hurt, Administrator

Laura Kelly, Governor

DATE: **July 26, 2021**

BULLETIN: **2021-KDCU-CUB-15**

TO: **Kansas Chartered Credit Unions**

SUBJECT: **Cybersecurity**

CYBERSECURITY

Kaseya. JBS. Colonial and DarkSide. And, of course, there will always be Target. Hard to believe it has been eight years since an HVAC company opened the online door to Target and, looking back, may have opened the floodgates to cyberattacks across the country.

By now, everyone knows about supply chains, right? If you read the news, you had to have noticed cyberattacks are now coming fast and furious (and I am not talking about the movie!). The United States critical infrastructure, which includes financial institutions, is a tempting target for ransomware. The importance of a credit union's cyber hygiene is not new as KDCU has published prior bulletins related to this topic.

Solar Winds. Microsoft. Pulse Connect Secure. If your credit union is connected to the internet, then your member data will be one of those tempting targets. KDCU staff have heard many a credit union indicate they were not worried as they were relying on their vendors. What happens when your vendor is victimized? When your member data is electronically downstream from that vendor? A credit union cannot contract away its regulatory responsibilities.

One cyber rating system vendor report found 48% of credit unions and 58% of their vendors could have "critical vulnerabilities due to out-of-date systems." Do not believe Kansas credit unions are immune to cyberattacks. KDCU examiners have found credit unions which have failed to keep up with basic software patches.

The Carnegie Endowment has published a timeline of cyber incidents involving financial institutions. Federal Reserve Chairman Jerome Powell has said he is on alert for cyber attacks, particularly those which could cripple a financial institution to the point payment systems do not function. Interpol is working on a new strategy to combat ransomware.

The National Credit Union Administration (NCUA) regulations, specifically Part 748 and appendices, instruct credit unions on safeguarding member information and response programs for unauthorized access to member data. NCUA also provides a cybersecurity resource page for credit unions.

If you have not done so, it is highly recommended you and/or your IT staff sign up for bulletins from the Cybersecurity & Infrastructure Security Agency (CISA). CISA provides timely information on attacks and software updates; and now offers a ransomware resource page.

Kansas credit unions are part of the financial infrastructure of the United States and, in many cases, process payments on a daily basis which are electronically transferred to hundreds of other financial institutions. As indicated by the information above, all eyes are focused on cybersecurity and it is more important than ever to stay cyber alert.