CYBERSECURITY
AWARENESS
MONTH

DO YOUR PART.
#BECYBERSMART

5 WAYS CREDIT UNIONS CAN BE CYBER SMART

October is National Cybersecurity Awareness Month, in which invaluable resources are shared to help credit unions reduce cyber risk in order to protect critical systems and secure confidential data. As your trusted compliance partner, we have outlined 5 ways that credit unions can support and enhance its cybersecurity culture.

1. **Understand your credit union's risk to cyber threats.** According to FFIEC and NCUA guidelines, credit unions should conduct Cybersecurity Risk Assessments to identify and understand your organization's strengths and weaknesses within IT Security and Cybersecurity Programs. Cybersecurity Risk Assessments should be performed at least annually, and should be used as a tool to enhance security controls over systems and data.

2. **Establish a culture focused on security.** Develop and implement an Information Security Program that encourages awareness of security best practices through policies and procedures. At least annually, ensure your Board and employees receive annual training of the credit union's Information Security and Cybersecurity Program. Communication is vital to the success of any organization's security programs – ensure employees are made aware of emerging threats and consider establishing processes to share cyber threat information with all stakeholders.

3. **Protect critical systems and confidential data.** Keep your systems and applications updated with the latest versions and patches. Implement strong security controls including, but not limited to, antivirus, intrusion detection and prevention solutions, password complexity and multifactor authentication settings, data encryption, and content filtering. Most importantly, access to systems and data should be granted based on job responsibility and requirement to perform job duties – periodically review user access to systems and applications to ensure access rights and permissions are still appropriate.

4. **Manage your third parties and vendors.** Establish a Vendor Management Program to encourage consistent and practical due diligence monitoring over third party relationships. Identify third parties that have direct and indirect access to critical systems and confidential data; and ensure strong controls are in place to safeguard against unauthorized access and misuse. System and application reports, including remote access logs, should be frequently reviewed to identify any suspicious or unusual activity.

5. **Test, adjust, and test again.** Ensure your Information Security and Cybersecurity Program outlines the requirements to continuously test controls and practices to ensure policies and procedures are effective. Annual IT testing programs should include an IT Audit, Information Security Risk Assessment, Internal and External Vulnerability Assessments, Penetration Testing, and Social Engineering Testing. Enhance your security programs based on the results of audits and assessments, and ensure periodic testing is performed to reassess the effectiveness of controls.

Not sure how to implement the 5 ways to be cyber secure?
Buckley Technology Group can help your credit union #BeCyberSmart.

For more information, visit **www.buckleytechgroup.com**

BTG
BUCKLEY TECHNOLOGY GROUP