COMPLIANCE SPOTLIGHT

Volume 1 / Issue 1 March 2022

UPCOMING EVENT

April 20th, 2022 – BTG will be exhibiting at CCUA's CU Marketplace held at DCU Center in Worcester, MA.

COMPLIANCE REMINDER

Updates to the Information Security Program Policies must be reviewed at least annually and presented to the Board for approval.

Contact Us

Buckley Technology Group
P.O. Box 530, Norwell, MA 02061
(800) 355-4550
sales@buckleytechgroup.com

www.buckleytechgroup.com

IS YOUR CYBERSECURITY FOCUS RELEVANT AND REALISTIC?

Following current global events, federal agencies have issued multiple alerts and guidance speaking to the potential increase of cyber attacks and incidents in which financial institutions could be targeted and impacted. The recent primary focus has been on the likelihood and impact of Ransomware attacks, and the need to establish resiliency and response safeguards. As a result, many of our clients are seeking solutions or are in the process of putting in place enhanced controls to monitor their networks and combat Ransomware.

Your cybersecurity focus should not have tunnel vision…

The FBI recently released its 2021 Internet Crime Report which shows that Business Email Compromise (BEC) is the dominant cyber threat. Business Email Compromise is a scam targeting businesses and individuals in which a transfer of funds scam is carried out when the target's business email account is compromised through social engineering or phishing attacks.

In 2021, Business Email Compromise scams resulted in nearly $2.4 billion in victim loss while Ransomware attacks resulted in a $49.2 million reported loss.

Business Email Compromise scams cost victims 49 times more than reported Ransomware attacks in 2021.

To be clear, Ransomware attacks are a very real threat that can have severe impacts. However, financial institutions should not lose sight of addressing additional relevant cyber threats.

Since Business Email Compromise scams begin with targeting employees through social engineering and phishing attacks, financial institutions should have a multifaceted approach to combat these threats…not only with the use of technical controls! Train your employees on email best practices and social engineering red flags. Then, test your employees' response and awareness through simulated phishing exercises.

If your institution has not effectively trained and tested your employees, are you really prepared for a cyber attack? Buckley Technology Group is a partner with KnowBe4, providing managed security awareness training and simulated phishing testing for financial institutions nationwide. Contact us for more information on our Employee & Board Awareness Training Programs and Social Engineering Testing engagements.

Elisabeth N. Esposito