ABA Insurance Services | MEMBER OF GREAT AMERICAN INSURANCE GROUP

SafeAlert™

The invasion of Ukraine has raised concerns about potential cyber-attacks

The current crisis unfolding in Ukraine has ramifications well beyond Eastern Europe. Cyber security experts and bank regulatory agencies are warning of the potential for a worldwide increase in disruptive cyber activity on two fronts: cyber-attacks on critical infrastructure organizations, and more widespread threats designed to take advantage of public interest and sympathy for the Ukrainian people.

While it has been reported there are currently no specific or credible threats to the United States, the Cybersecurity and Infrastructure Security Agency (CISA) recently issued a "Shields Up" advisory (www.cisa.gov/shields-up) outlining steps every organization can take to detect and mitigate potential cyber-attacks.

CISA recommends all organizations increase vigilance now as threat actors have the ability to quickly distribute attacks at scale. Among the organizational guidance, CISA's specific recommendations include:

- Validation that all remote access to an organization's network and privileged or administrative access requires multi-factor authentication
- Confirmation that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes
- Testing backup procedures to ensure that critical data can be rapidly restored if the organization is impacted by ransomware or a destructive cyber-attack and ensuring that backups are isolated from network connections.

The advisory also provides a number of recommendations for corporate leaders and CEOs, as well as ransomware response tips and steps you can take to protect yourself and your family.

Unfortunately, whenever there is an event of mass impact, cyber criminals use our caring instincts against us to distribute malicious content and malware, often through phony websites and bogus charitable scams.

As always, staff awareness and education are critical as people are the most vulnerable entry point for cyber-attacks. In addition to your bank's regular, ongoing training, now is the time to remind your staff to think before they click on links embedded in email and text messages. According to the "Shields Up" advisory, 90% of successful cyber-attacks begin with a phishing email.

It's also important to stick to established sources for online news and only donate through reputable charities. Finally, keep passwords strong and secure and use MFA whenever possible.

You can access additional loss control resources on a variety of topics such as cybersecurity, wire fraud, employment practices and more on ABA Insurance Services' blog at Insights on abais.com To subscribe to SafeAlert, request reprints or if you have questions about this newsletter or articles, contact marketing@abais.com or 800-274-5222.