County Reinsurance, Limited

September Edition

Employee Awareness: Reporting Suspicious Activity

Welcome to the seventh installment of the eRisk Cyber Campaign!

Each month, these updates will go to the Member Designated Representative and your assigned eRisk Hub key contact. If you haven't named one yet, please send their information to **crl.memberservices@countyre.org.**

Help your counties take full advantage of what's available. Tap into CRL's resources to better manage risk. Your involvement ensures we move forward together, stronger and more prepared.

Cyber Incidents Happen. Here's What You Need to Do.

An employee notices unusual pop-ups and file behavior on their workstation but is unsure whom to contact. Delayed reporting allows the ransomware to spread to shared drives. Quick reporting could have contained the outbreak.

No security system is perfect—quick reporting is critical in limiting damage from a cyberattack.

- Learn how to recognize and report suspicious activity.
- Follow our internal reporting protocols to ensure threats are handled

efficiently.

Reminder for IT Managers: Review your Cyber Risk Profile to confirm that incident reporting processes are clearly documented and enforced.

The entire Cyber Resilience series is available today. To learn more and/or complete these actions, log into the eRiskHub to visit the Cyber Resilience page.

Please contact **crl.memberservices@countyre.org** with general questions regarding the campaign. For technical questions concerning the eRiskHub portal, contact Net Diligence at **eriskhub@netdiligence.com**.

August Email: IT & Management: Phishing Tests & Employee Readiness