

Ransomware attacks are on the rise and can bring in massive losses of \$5 million or more. Your insureds may need Excess Cyber Liability coverage and additional Loss Prevention Protections to ensure they are covered.

Phishing emails are one of the most commonly used ways of initiating ransomware attacks. Catching phishing emails before they are opened is one of the keys to cutting down on bad actors' ability to carry out these attacks via ransomware (malware).

PROFESSIONAL LIABILITY RANSOMWARE & EXCESS CYBER LIABILITY



It is also important for your insured to have the following protections in place:



Multi-factor authentication (MFA)



Good patch management



Backups (not attached to the insured's network)



Secure email gateway (SEG)



Disable macros

- Backup is stored off-site
- Backup is stored in the cloud

Reach out to one of our brokers today for excess cyber options for your insured!

Alec Immordino

ext 8784 | aimmordino@arlingtonroe.com

Essie Bennett

ext 2260 | ebennett@arlingtonroe.com

John Immordino

ext 8732 | jimmordino@arlingtonroe.com

Mark Swayze

ext 8648 | mswayze@arlingtonroe.com

Melissa Hilgendorf

ext 8774 | mhilgendorf@arlingtonroe.com

Sarah Immordino

ext 8731 | simmordino@arlingtonroe.com

Shelly Caldwell

ext 8687 | scaldwell@arlingtonroe.com

Sonya Townsend

ext 8668 | stownsend@arlingtonroe.com