Cyber Liability – 6 Trending Issues

Trending Issue:	Action Plan:
Deepfakes Deceive Us There are at least **14,678** deepfake videos online, according to Deeptrace.	• Watch out for deepfake videos spreading fake news • Don't add to the problem. Check for authenticity before you share videos • Beware of fraudsters using deepfake videos in social engineering schemes
Ransomware Gets Sophisticated New ransomware attacks increased **118%**, according to a McAfee 2019 report.	• Use secure networks, strong passwords and up-to-date systems • Learn how to identify and avoid malicious links • Maintain secure backups of essential files
IoT Devices Provide Access Smart speakers, smart fridges, smart everything. Gartner says there will be **25 billion** connected things by 2021.	• Don't use the factory settings. Pick a strong password and check privacy settings and permissions • Check smart devices for security problems and updates regularly • Consider setting up a separate network for smart devices
Data Privacy Laws Take Effect Businesses may spend **$55 billion** to comply with CCPA, California's new data privacy law. Compliance with New York's SHIELD Act is also required effective March 21, 2020.	• As big data grows, privacy concerns are also growing • Data breaches can put sensitive information in the hands of identity thieves • Keep up with the new data privacy rights and requirements, including CCPA, GDPR and the SHIELD Act
Spear Phishing Gets Personal **91%** of cyberattacks start with a spear fishing, according to Cofense.	• Train your team to not click on links unless they are positive that they trust the source • Watch out for messages that appear to be from people you know but are actually spoofed • Use anti-virus software, two-factor authentication and other security measures
Employees Let the Bad Guys In The Verizon Data Breach Investigations Report found that human mistakes caused **21%** of data breaches in 2018.	• Train your employees on how to avoid phishing and other cyberattacks • Make sure remote workers are using strong cybersecurity protocols • Change passwords after employees leave