RISK ALERT
While everyone’s priority is to obviously focus on personal hygiene and safety, there are bad actors taking advantage of the COVID-19 pandemic for personal gains. Below are a few things to be aware of as well as best practices on the cyber/privacy hygiene front:

- Risks & exposures (adapted from Lockton’s recent COVID-19 webinar)
  - Remote workforce
    - Reliance upon VPNs and other remote applications may not support the bandwidth and other productivity levels - system failure of the organization’s infrastructure or SaaS provider could result
    - Testing should be conducted to ensure systems are able to accommodate increased remote workforce
    - Home and personal work stations are often less secure and more susceptible to hackers
  - Data collection & privacy
    - Companies may be careless in sharing information they have regarding affected employees and others - privacy breaches could violate HIPAA, state laws and company privacy laws
    - Companies may react to the epidemic by requesting information from customers, vendors and employees that they are not entitled to ask for
  - Phishing
    - High-profile global issues and crises are perfect fodder for hackers; using the coronavirus theme for phishing emails or other predatory techniques is prevalent
  - Business Interruption
    - Interrupted suppliers and targeted attacks knowing the control rooms aren’t staffed adequately can result in easier prey from an adversary standpoint
    - A company’s inability to operate and maintain its systems because of a quarantine or shutdown could potentially trigger business interruption coverage; unintentional or unplanned system outage coverage could be invoked but will most likely be aggressively disputed by insurance carriers

- Be aware!
  - Johns Hopkins has been a leading source of COVID-19 data but we are now seeing imposter sites take information and infect users - https://www.americanbanker.com/news/coronavirus-scams-to-watch-out-for
• Best practices
  
  o Avoid clicking on links in unsolicited emails and beware of email attachments. Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Attacks
  
  o Use trusted sources—such as legitimate, government websites—for up-to-date, fact-based information about COVID-19.
  
  o Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
  
  o Verify a charity’s authenticity before making donations. Review the Federal Trade Commission’s page on Charity Scams for more information.
  
  o Review CISA Insights on Risk Management for COVID-19 for more information.