

# AGENDA

Ransomware/Extortionware

## CISO Council

### SPEAKERS



**Leo Cunningham**  
ASO  
[Flo Health Inc.](#)



**John Williams**  
VPSecurity  
[Korn Ferry](#)



**Steven Gilham**  
Infrastructure Security  
Manager  
[TSB](#)



**Nicolas Groh**  
Field CTO, EMEA  
[Rubrik](#)



**Leo Cunningham**  
ASO  
[Owkin Inc](#)

[CLICK HERE TO REGISTER](#)



**January 17, 2023**  
11:00 AM-12:00 PM  
United Kingdom Time

### Ransomware/Extortionware

CISOs face a huge headache trying to understand how to know when they were attacked, what data attackers have corrupted? How quickly can they recover from the attack? And do they have to pay a ransom to get the data back? Ransomware remains a significant challenge for companies, not simply because it has become ubiquitous, but also because of the significant impact a single ransomware attack may have on a company and every other company or customer that relies on that company. Cybersecurity and risk management have always been vital for the flow of any business. However, the current condition of the global supply chain makes it exceptionally vulnerable to severe damage from an attack more so than usual. When the supply chain is barely getting by, criminals are more likely to assume they have leverage over businesses. A ransomware attacker may be more brazen and exercise higher demands than they might have a few years ago

## PANELISTS



Chair

**Leo Cunningham**  
**CISO**  
Flo Health Inc.



Chair

**Leo Cunningham**  
**CISO**  
Owkin Inc



Speaker

**Steven Gillham**  
**Infrastructure Security**  
**Manager**  
TSB



Speaker

**Nicolas Groh**  
**Field CTO, EMEA**  
Rubrik



Speaker

**John Williams**  
**VP Security**  
Korn Ferry

TOGETHER WITH

