Executive Briefings

- History of Russia and Ukraine (from Wikipedia)

Board Briefings

- 10-15 minutes
- Risk posture
- Exposures
- Compensating Controls
- Overall security plan

Administrative Controls

- Travel/Evacuation policies
- Asset disposal
- Data lifecycle
- Crown jewels

Technical Controls

- Firewalls
- GeoLocation blocking
- Monitor VPN connections
- UERA
- MFA

Team Analysis

- SWOT Analysis

- Strengths
- Weaknesses
- Opportunities
- Threats

Business Analysis

- PEST Analysis

- Political
- Economic
- Social
- Technical

News Resources

- SANS ISC
- SANS Webinar
- TrustedSec Discord
- BHIS Discord
- Technical Resources

SANS ISC

CISO Actions - Russia/Ukraine Activity

- December 2015
  - Attacks using the Trojan virus BlackEnergy on energy companies in Ukraine which provide energy to Kyiv, Ivano-Frankivsk, and Chernivtsi regions
- Power Grid Attack
- This was the first successful cyber attack on a power grid
- Second Ukraine power grid hack, December 2016
- Paralysis of the State Treasury of Ukraine, December 2016
- According to the US Presidential Administration, this attack became the largest known hacker attack.
- 2022 Ukraine cyberattack, attacks on Ukrainian government websites, January 2022, one day after US-Russian negotiations on Ukraine's future in NATO failed
- Attacks in February 2022, after Russian troops invaded eastern regions of Ukraine, took down several major Ukrainian governmental and banking websites. U.S. intelligence attributed the attacks to Russian attackers, although the Russian government denied involvement

Business case if needed

Board Briefings

- 10-15 minutes
- Risk posture
- Exposures
- Compensating Controls
- Overall security plan

CISO Actions - Russia/Ukraine Activity