CONNER STRONG & BUCKELEW

CYBER BULLETIN

RUSSIA INVASION

Cyber Security & Liability Impacts

The Russia invasion of Ukraine may have cascading effects to businesses and institutions as targeted cyber disruptions transcend physical borders. Cyber-attacks aimed at large competing economies may have direct impact to your operations and bottom line. The origination and affiliations of responsible actors are not always readily apparent. The perpetrators and their intent may have implications as to how cyber policies respond to claims.

The Ukrainian crisis coupled with an already challenging cyber liability market underscores the importance of working with a broker that understands the nuance of policy coverages. We also recommend an emphasis on cyber security protocols to mitigate the risk of an adverse event from crippling your business or institution. Cyber security is a complex and ever evolving discipline, but following are some basic program elements that cyber insurers are setting as a minimum standard to secure coverage and receive the best terms and conditions.

- Backups of your data and systems that are segregated and secured
- Utilize a Virtual Private Network (VPN) and Multi Factor Authentication (MFA) for all remote connections
- Utilize endpoint detection and response (EDR) and Next Generation Anti-Virus
- Security monitoring that correlates computer and user events on endpoints, across the network, in applications, and the cloud
- Know your assets and practice good maintenance of all systems and data

- Protect your borders – firewall enabled on all active ports, unused ports closed, antivirus and antimalware enabled for network servers that connect to the internet
- Additional controls to secure all privileged accounts and online services, such as Privileged Access Management and password vaults
- Train and test employees on common types of attacks (e.g. phishing emails)
- Have an incident response

BOTTOM LINE: READ YOUR POLICY, TALK WITH YOUR BROKER AND SECURE YOUR SYSTEMS.

Be sure and include your internal IT and cyber security teams in cyber risk management discussions, and please contact your Conner Strong team for additional information.

Cyber Threat Landscape

Conner Strong has been working with various threat intelligence sources to ensure we can provide you data to shed light on how current events may impact your business.

Below are some sobering facts that experts agree may lead to an increase in risk for all US entities:

- A recent decline in ransomware leading to the invasion is evidence of Putin's ability to control world ransomware activity, and the connection between Russian Intelligence services and cybercrime.
- This reduction is expected to reverse in the coming three (3) weeks to a month as Russian intelligence along with their cybercrime counterparts resume the deployment of new sophisticated attack campaigns.
- Russian intelligence has recently "cracked down" on criminal organizations within Russia but may in fact incorporate some of those criminal actors into current military operations
- REvil ransomware group (Ransomware Evil) is the 2nd highest operational tempo cybercrime group.
- It is believed by most experts that Putin will attempt to disrupt infrastructure and economies worldwide by unleashing ransomware and malware not meant for cybercrime profits but only to negatively affect Ukraine's allies, e.g., ransomware for which paying a ransom will not decrypt the data.
- Non-governmental cybercrime actors, independent actors, Anonymous, and hacktivists have complicated these events, and either have, or have claimed to have joined in the cyberwar. Much of this activity has no formal direction from Russia, Ukraine, or other governments, and is spurring what may be the first cyberwarfare free-for-all. These groups may generate unintended impacts on businesses and organizations worldwide.

Read detailed information on Russian state-sponsored cyber threats to U.S. critical infrastructure published by CISA.

CONNER STRONG & BUCKELEW