PROTECTING AGAINST CYBER THREATS DURING THE RUSSIA-UKRAINE CONFLICT

By **Brooke Watson**

"Most of America's critical infrastructure is owned and operated by the private sector and critical infrastructure owners, and operators must accelerate efforts to lock their digital doors." – President Joe Biden, March 21, 2022

On March 21, 2022, the Biden administration released a statement emphasizing a prior warning "about the potential that Russia could conduct malicious cyber activity against the United States, including as a response to the unprecedented economic costs [the United States has] imposed on Russia" and "reiterating those warnings based on evolving intelligence that the Russian Government is exploring options for potential cyberattacks."

While the Russian invasion of Ukraine and the resulting sanctions imposed on Russia may be contributing to an uptick in cyberattacks, Russia has long been a primary source of cybercrime. As of October 2021, Microsoft reported: "During the past year, 58% of all cyberattacks observed by Microsoft from nation-states have come from Russia." Although the threat of Russian cyber incidents has long been prominent, Russia's recent actions have highlighted these cybersecurity concerns and brought them to the forefront of Americans' minds.

There is no doubt that the likelihood of U.S.-based organizations experiencing malicious cyber incidents at the hands of Russian cybercriminals will increase due to Russia's conflict with Ukraine. As a result, leaders in business and government must act with urgency and enact measures to protect against such attacks, including the following:

Engaging proactively with local law enforcement, including the local Federal Bureau of Investigation (FBI) field office or Cybersecurity and Infrastructure Security Agency (CISA) regional office to establish relationships in advance of any cyberattack;
Implementing security measures that continuously monitor and identify potential threats;

- Requiring the use of multi-factor authentication on an organization’s systems to prevent intrusion by a bad actor;
- Implementing data encryption so data cannot be used if it is accessed by a cybercriminal;
- Conducting personnel training to identify suspicious emails, websites, links and behaviors, and encouraging employees to notify those in an organization who can properly investigate any suspicious activity if experienced;
- Developing patching strategies and consistently and timely implementing such patching strategies, in conjunction with cybersecurity professionals, particularly against known vulnerabilities, including standard protocols to evaluate, develop and apply patches to the organization’s systems, or creating contractual commitments for a vendor to do so if the company or governmental entity relies on a third party to maintain its computer systems;
- Requiring all system-wide users to choose a new complex password;
- Developing and maintaining proper security policies tailored to the organization that focus on the most critical data;
- Making the organization’s security policies manageable and accessible to all employees;
- Developing and testing an incident response plan, which can aid an organization in responding promptly and minimizing a cyberattack’s effects;
- Backing up data in another location that would not be accessed by a malicious actor if the system is breached, and implementing regular offsite backups combined with a business continuity plan;
- Engaging proactively with cybersecurity legal counsel prior to an organization experiencing a cyber incident; and
- Obtaining cyber insurance.

Due to the turmoil and general unrest occurring as the result of the Russia-Ukraine conflict, cybercriminals (particularly those in Russia) have identified yet another opportunity to prey on U.S. organizations, which may be making swift decisions or experiencing tightly stretched resources. Unfortunately, there is no means to ensure that an organization is completely protected from a malicious cyberattack.

However, rather than waiting for an event that increases an organization’s vulnerability to a cyber incident, or worse, waiting for an attack to occur, it is important to proactively manage cybersecurity risks. While implementing cybersecurity measures can require an organization to contribute substantial resources, implementing the security measures identified above can lower an organization’s vulnerability to a cyberattack, both during the present Russia-Ukraine conflict and in the future.