MARCH 3, 2022

Ukraine-Russia Conflict Demands Heightened Cybersecurity Vigilance

By Clifford Forrester, CIO

The Ukraine-Russia conflict has raised the very real possibility of reprisal cyberattacks by Russian government-sponsored threat groups and threat actors with a pro-Russia agenda. There have been many reports of denial of service and wider cyber-attacks impacting Ukrainian government entities and financial institutions. In response to stringent Western government sanctions against Russia, there is also the potential for an increase in phishing emails and ransomware that will be more dangerous and disruptive than ones previously encountered.

In this volatile and dangerous environment, the need for vigilance in your cybersecurity posture has never been more urgent. Here are some key reminders to protect your organization and yourself.

REDUCE THE LIKELIHOOD OF A DAMAGING CYBER INTRUSION

- Require that all remote access must have multi-factor authentication (MFA)
- Make all software updates – especially ones that address known exploited vulnerabilities
- Confirm that your IT personnel have disabled all ports and protocols that are not essential
- Initiate strong cloud services controls

TAKE STEPS TO DETECT A POTENTIAL INTRUSION QUICKLY

- Identify and assess unexpected and unusual network behavior
- Confirm that the organization's network is protected by antivirus/antimalware software
- If working with Ukrainian or Ukraine-friendly organizations, take extra care to monitor, inspect, and isolate network traffic

ENSURE THAT THE ORGANIZATION IS PREPARED TO RESPOND IF AN INTRUSION OCCURS

- Designate a crisis response team with main points of contact for suspected incidents and roles/responsibilities
- Assure availability to key personnel; identify means to provide surge support responding to an incident
- Conduct tabletop exercises to ensure that all participants understand their roles during an incident

MAXIMIZE THE ORGANIZATION'S RESILIENCE TO A DESTRUCTIVE CYBER INCIDENT

- Test backup procedures to ensure that critical data can be restored rapidly if the organization is impacted
- Conduct a test of manual controls to ensure that critical functions remain operable

STEPS YOU SHOULD TAKE AS AN EMPLOYEE AND IN YOUR PERSONAL LIFE

- Be vigilant and operate with a healthy dose of skepticism with your online interactions
- Watch for emails soliciting donations for Ukrainian relief
- Verify the URL of any link before you click on it by hovering your cursor over the link and examining the URL. If you don't recognize it, don't click on it
- Delete any suspicious emails and contact your IT Service Desk
- Don't enter your credentials (especially your company UserID) to access any website if you are not **1000%** sure of its validity
- Remember, not all client or vendor websites are safe, so don't operate with blind trust

For more insights on enhancing your cybersecurity and infrastructure protection, visit **Shields-Up Guidance from the US Government (https://www.cisa.gov/shields-up).**

If you have any questions, please contact Clifford Forrester, Chief Information Officer and Leader of **Berdon's Technology Services** (BTS) Practice, at 212.699.6710 | cforrester@berdonllp.com. BTS provides information technology solutions, including cybersecurity advisory, to businesses across multiple industries.

Clifford Forrester *brings more than 20 years of professional experience to his role as the firm's Chief Information Officer.*

Berdon LLP is a full-service accounting and advisory firm which also offers specialized services such as state and local tax, trust and estate planning, family office services and business valuations. For more than 100 years, Berdon has served a variety of clients, including some of the nation's premier family-owned real estate companies, international law firms, advertising, architecture, and engineering/construction firms and noted figures in the arts and entertainment industry.

BERDON LLP | 360 Madison Avenue, New York, NY 10017 | 100 Jericho Quadrangle, Jericho, NY 11753 |