How the War in Ukraine Could Increase the Risk of Cyberattacks

Cybercrimes have wreaked havoc on businesses since before the invention of the computer, so the risk is nothing new. However, Russia's invasion of Ukraine has brought the fear of cyberattacks to the forefront in recent weeks.

"We need to be prepared for the potential of foreign influence operations to negatively impact various aspects of our critical infrastructure with the ongoing Russia-Ukraine geopolitical tensions," Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly said in a statement. "We encourage leaders at every organization to take proactive steps to assess their risks from information manipulation and mitigate the impact of potential foreign influence operations."

Credit professionals need to not only be aware of the risk of cyberattacks on their own business, but also those of their customers and banks. "Companies need to recognize that this isn't a situation that's going to end in days or weeks," former National Security Agency Director Adm. Michael Rogers told Kellogg Insight.

Rogers warned that certain industries and types of companies are at a greater risk of falling victim to Russian ransomware attacks than others. For example, economic infrastructure, military, financial institutions, electric and businesses "uniquely associated with America" (Coca-Cola or McDonald's) could be main targets of these attacks.

Hackers who carry out these attacks generally have one of two common goals—either to lock down your company's system until you pay them for access, or to steal intellectual property. "The threat-level varies by sector," Rogers explained. "So, from an intellectual-property standpoint, if you're in the high-tech, energy or defense areas, you're an attractive target."

This becomes an issue for credit professionals who store highly sensitive personal and financial information. It is also a problem if your customers' business systems are shut down and may not be able to pay. "With so much focus on Ukraine, this could be a time that the U.S. could be more vulnerable to cyberattacks," said Brett Hanft, CBA, credit manager with American International Forest Products, whose company has been hit by a cyberattack in the past. Add into the mix remote workforces, which make it easier for cyberattacks to obtain or wipe out personal and work information in one location, Hanft added.

Credit professionals should take the following proactive steps to protect highly sensitive credit information:

- Create new and strong passwords
- Verify where emails are coming from and think before you click
- Require multifactor authentication for especially sensitive documents
- Store a backup of documents on a thumb drive or other external device
- Ensure all software is up to date
- If working with Ukrainian organizations, take extra care to monitor, inspect and isolate traffic from those organizations and closely review access controls for that traffic (CISA)

At NACM's 126th Credit Congress & Expo, Hanft will share tips and best practices he learned firsthand when his company experienced a cyberattack. Check out, Cyber-Attack: A Different Perspective When It Happens to YOU!