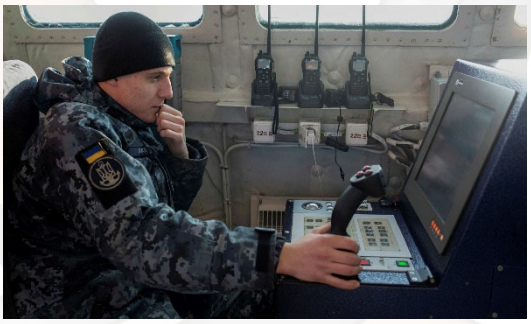
Ukraine Invasion Heightens Contractors' Risk of Cyberattack



Cybersecurity experts around the world are sounding the alarm about a potential increase in Russia-led cyberattacks following the country's Feb. 24 invasion of Ukraine, and some say the construction industry could be a target.

According to CNN, U.S. officials are concerned that the incursion could spill over into cyberspace, and warned businesses, banks and local governments about being vigilant against threats. Construction companies should be on high alert as well, according to Raymond Monteith, senior vice president with HUB International Limited's risk services division.

"Small and medium-sized enterprises, which contractors often fall into that realm, are among the most targeted organizations, and often that is because they're especially vulnerable to cybersecurity attacks," he said. "Largely because of a lack of resources, they often don't have dedicated IT individuals, they don't have the internal resources that can be focused on building and maintaining and monitoring robust cybersecurity and defensive systems, so they are frequently targets and do have some significant vulnerabilities."

Construction has been documented as particularly vulnerable to cyberattacks such as ransomware, a type of program that can steal or encrypt sensitive files and information and demand compensation for their return or safety. Construction was the top industry hit by ransomware attacks in 2021, according to a December report from encryption software firm NordLocker, which analyzed 1,200 companies across 35 industries.

Ransomware attacks can target firms of any size, from family-owned contractors to global giants. The proliferation of new technologies in the industry also means more potential vulnerabilities. These kinds of attacks don't start out, however, with criminals in masks hiding behind monitors filled with lines of code actively "hacking the mainframe," but rather from ordinary people clicking a bad link or exposing their information, he said. "Generally speaking, ransomware and business email compromise are what we would term 'public enemies No. 1 and 2' these days," Monteith said.

How To Secure Data

Countries are responding to the possibility of increased cyber threats from Russia. In the U.K., new cybersecurity guidance for contractors, launched by Britain's National Cyber Security Centre along with the Chartered Institute of Building, aims to help small and medium-sized contractors use new technologies safely. "By following the recommended steps, businesses can significantly reduce their chances of falling victim to a cyberattack and build strong foundations for their overall resilience," said Sarah Lyons, NCSC Deputy Director for Economy and Society Engagement, in the press release.

Some of the NCSC's cybersecurity guidance for contractors includes avoiding common passwords or using a default password and being careful about what information is posted on social media. The group also recommends that construction firms enable two-factor authentication, where a separate channel, such as an email or a phone number, is used to verify new logins or other security issues on company accounts.

"Due to online threats facing the sector, the NCSC advises firms that cyber security measures are as vital as wearing a hard hat on site," the NCSC said in the release.

Stateside, New York Gov. Kathy Hochul and New York City Mayor Eric Adams, along with the mayors of other large cities in New York State, unveiled the creation of a Joint Security Operations Center (JSOC) last week. Hochul said last week at a press conference that the state's institutions, governments and critical infrastructure, which includes water, transportation and power sources, were all vulnerable to attacks, Smart Cities Dive reported.

Phil Casto, senior vice president for risk services at HUB international, wrote last year about some other steps contractors can take:

- Train employees.
- Keep software up to date.
- Dispose of technological assets properly.
- Give your company an annual cybersecurity checkup.
- Purchase a cyber insurance policy.

"Cybersecurity is never a one-and-done event. It is a continual process," Security experts agree that in today's landscape it is not a question of if but when, and being prepared is the key.

Matthew Thibault
Associate Editor – ConstructionDive