BLANKROME

Cybersecurity & Data Privacy

MARCH 2018 • NO. 1

Be Advised—Russian Cyber Activity against Critical Infrastructure Sectors

The U.S. Department of Homeland Security ("DHS") and the Federal Bureau of Investigation ("FBI") have released information regarding cyber activity by the Russian government against organizations involved in critical infrastructure sectors. Organizations in the energy and maritime industries and those that operate in critical infrastructure sectors must be alert and actively review and assess their cybersecurity defenses, breach response plans, and information security protocols.

WHAT YOU NEED TO KNOW

According to the DHS and the FBI, since about March 2016, Russian cyber attackers have actively targeted organizations involved in various critical infrastructure sectors. In particular, this campaign targeted entities in the supply chain for these sectors, some of which may not have sound cyber protections in place. Suppliers often have connectivity and access to important systems within larger, better protected organizations, their true target. Organizations in the energy and maritime industries should review their relationships with critical infrastructure entities to determine if there is sufficient integration where they may be targeted.

This campaign has utilized a multi-stage attack process designed to obtain access to systems through attacks as simple as phishing. Once the attacker has access, they use more advanced techniques to move throughout a network to obtain information, particularly regarding industrial control systems, such as plant automation, management, and control systems.

Blank Rome recommends that organizations take the following steps to protect themselves:

- Review the linked US-CERT alert, which contains detailed technical information to your relevant management, security, and IT staff: TA18-074A: Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors;
- Ensure your organization has an effective information security program in place, including keeping systems up-to-date, as well as rapid threat detection and response capabilities;

- Communicate with your employees to ensure they are well-trained to detect and properly respond to e-mail-based attacks, such as malicious links or attachments in e-mails that may appear to be sent from known parties; and

- Ensure that your suppliers that have access to information regarding your systems, or have access to your systems, have sound information security practices in place, such as facility management, IT, mechanical, plant management, and transportation service providers.

Blank Rome is your partner in protecting the energy, maritime, and critical infrastructure industries. Please contact us if you have any questions about implementing these steps or any other cyber issues impacting your organization, such as assessing risk, preparing defensive programs, or responding to a security breach.

For more information, please contact:

Kate B. Belmont, Maritime
212.885.5075 | kbelmont@blankrome.com

Jennifer J. Daniels, Cybersecurity & Data Privacy
212.885.5575 | daniels@blankrome.com