Updates
March 29, 2022

Recent Warnings Highlight Need for Enhanced Cybersecurity of Critical Infrastructure

The U.S. government has steadily increased its warnings about malicious cyber activity by Russia and other sophisticated persistent adversaries. Following several warnings from the Federal Bureau of Investigation (FBI) and the U.S. Department of Homeland Security (DHS), the White House on March 21, 2022, committed to deploy federal resources to protect against such attacks and highlighted the important reality that "much of the Nation's critical infrastructure is owned and operated by the private sector and the private sector must act to protect the critical services on which all Americans rely."

The U.S. Department of Justice (DOJ) on March 24, 2022, unsealed two indictments of Russian government actors who targeted the global energy sector with malicious cyber activity. As alleged in the indictments, their attacks were designed to give the Russian government the ability to disrupt and damage industrial control system (ICS) and operational technology (OT) resources in a manner that could cause not only an interruption of service, but also potentially catastrophic physical effects. One of the indictments alleges that an individual who targeted U.S.-based oil refineries had previously used similar methods to intrude into the systems of a non-U.S. refinery, which triggered an emergency shutdown.

These indictments, combined with current events in Ukraine, shine a spotlight on the threat that confronts critical infrastructure providers. One indictment alleges that a Russian Ministry of Defense laboratory with a history of developing cutting-edge weapons produced and used malware that would allow an unauthorized actor to take control of safety systems and controllers. The indictment further alleges that the charged defendant and co-conspirators deployed the malware at an overseas company's refinery and then attempted to compromise a U.S.-based corporation that operates multiple refineries. The defendant's and co-conspirators' malware went beyond what an actor would need to merely shut a plant down and, as alleged, "could be employed to cause property damage, economic herm, as well as physical injury and death."

The other indictment alleges a year-long campaign by Russia's Federal Security Service (FSB) to use supply chain, spear phishing, and watering hole attacks to build the covert capability to, among other things, disrupt and damage the systems of hundreds of energy-related entities around the world. As set forth in the indictment, the conspirators installed malware on more than 17,000 devices globally, including ICS controllers used by power and energy companies.

The fact that critical infrastructure presents unique cybersecurity risks—risks that extend into the physical world—has been clear for some time. The ability of nation-state and other sophisticated malicious actors to exploit cyber vulnerabilities is similarly well known. These indictments, however, demonstrate that the cyber threat confronting critical infrastructure is not hypothetical. Rather, even before the invasion of Ukraine, Russian forces were devoting substantial time, expertise, and resources to compromising U.S. critical infrastructure using multiple vectors and preparing potentially catastrophic destructive attacks.

U.S. critical infrastructure companies and their vendors accordingly should take this threat seriously and work with security and legal partners to ensure that they are appropriately defending themselves. The U.S. government has recently issued updated guidance for critical infrastructure and other industries seeking to mitigate the Russian cyber threat in particular, including these posts: (1) Russia Cyber Threat Overview and Advisories, (2)

Alert AA22 – 011A, (3) Shields Up Technical Guidance, and (4) Private Industry Notification.

Relatedly, the recent enactment of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 should prompt critical infrastructure companies to closely examine their security and incident response postures. Similarly, the U.S. Securities and Exchange Commission's (SEC) proposed Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure rule will impose enhanced and standardized reporting requirements pertaining to both preparedness and incidents. Companies' efforts to build resilience against increasingly sophisticated attacks and to comply with new government requirements will require legal expertise in data security, litigation, interactions with law enforcement and regulators, and sector-specific considerations.

For all matters related to cybersecurity, response planning, incident response, reporting requirements, incident-related litigation, and engagement with government agencies, companies should consult with experienced counsel.

Authors

David Aaron

Senior Counsel
DAaron@perkinscoie.com

Explore more in

Privacy & Security | Technology Transactions & Privacy Law | Communications | Energy Infrastructure & Clean Technology

Related insights

Update

Employers and Immigration Under Trump: What You Need To Know

Update

‘Tis the Season… for Cybercriminals: A Holiday Reminder for Retailers