Government too leaky on grid cybersecurity threat information

COMMENTARY

BY PAUL TIAO AND ERIC HUTCHINS

The New York Times recently reported that it obtained a joint FBI and Department of Homeland Security (DHS) report that indicated that hackers have been targeting companies operating energy facilities and manufacturing plants across the United States and in other countries. That press account identified one such target, the owner of a nuclear power plant, specifically by name, quickly sparking public debate and alarm about the state of energy sector cybersecurity, particularly at nuclear power plants.

That public discussion is a continuing one, but it has not addressed a related fundamental question for critical infrastructure owners and operators and other private entities about sharing sensitive cybersecurity information with the federal government: Why do we know any of this in the first place?

To be clear, any fault here lies with those handling the joint report, not the New York Times, which simply reported information it obtained. Notably, the Times reported that the joint report “carried an urgent amber warning, the second-highest rating for the sensitivity of the threat.”

This characterization is not precisely correct, but the underlying information is vital. An amber warning is the second-highest rating within the government’s “traffic light” (TLP) system, but it relates to the sensitivity of information, not necessarily the urgency of a threat. Ironically, had those handling the joint report followed that amber designation, it would never have been made public.

This highlights the conundrum of information-sharing in the face of growing cyber-threats. The government wants to share threat information with potential targets. But too wide a distribution could compromise information, putting it in the hands of bad guys and undermining the environment of trust necessary for future sharing. There is an important sweet spot to hit, and the government missed it badly here.

TLP is used by government agencies to provide a simple format to indicate when and how information can be shared. TLP designations come in four varieties, each carrying more stringent handling expectations: (1) TLP: WHITE (public information); (2) TLP: GREEN (limited sharing); (3) TLP: AMBER (restricted sharing); and (4) TLP: RED (highly restricted sharing).

To understand TLP, it is important to know what it is not. TLP is not classified information with enforceable restrictions against disclosures, like “TOP SECRET.” TLP is not a congressionally-created designation with statutory exemption from disclosure or prohibition on regulatory use, such as DHS’s “Protected Critical Infrastructure Information” or designations under the Cybersecurity Information Sharing Act of 2015 (CISA). Nor is TLP one of the many “sensitive-but-unclassified” designations created by agency regulations.

In fact, TLP lacks any protections or special requirements, which is why it is so versatile. TLP basically tells recipients when to keep a secret, and is as effective as the procedures that implement it.

With this in mind, information directly identifying targets of a cybersecurity attack should not be marked less than TLP: RED, if it is disclosed at all. Even a restricted audience can prove too wide a circle for sensitive information—as seen with the joint report’s leak.

DHS is generally very cognizant of the importance of source-anonymization. For example, its guidance implementing CISA states that DHS will anonymize cybersecurity information shared with its National Cybersecurity & Communications Integration Center through the Automated Indicator Sharing initiative.

Yet even when content is not company-specific, information can be equally sensitive by virtue of its context. Thus, the appropriate TLP designation alone may sometimes not be enough and other steps may be necessary to limit access to designated information.

Ultimately, TLP is not about colors, it’s about developing trust to facilitate more frequent and effective collaboration—while protecting the underlying information. Press accounts discussing specific company names and a TLP-marked sensitive report chill that trust. The underlying “who said what” does little to comfort private sector entities sharing information with the government, and nothing to pull back security blueprints now possessed by threat actors.

Unfortunately, the electric sector has seen the inappropriate release of other cyber-threat information with specific target names before. Last December, for example, a Vermont utility responsibly shared information with the government identifying limited cyber-indicators on its systems potentially related to Russian malware—only to have officials incorrectly tell the press that Russians had hacked that utility.

Thankfully, these examples are the exception rather than the rule. In fact, public-private information sharing is conducted in a responsible manner to effectively mitigate cyber-threats. Nevertheless, they show areas for improvement of the handling of sensitive information by the government and offer important lessons to private entities sharing that information.

If not carefully controlled, well-intentioned information-sharing can result in unanticipated consequences. Thus, it is important that lawyers be involved in reviewing the types of information shared, creating sharing agreements and even approving the sharing of specific sensitive information. And when companies learn of an imminent or occurring compromise, lawyers can help mitigate resulting legal liabilities and reputational harms.

News of the joint FBI-DHS report reminds companies to prepare for increasingly sophisticated cyber-attacks. Indeed, this particular threat is ongoing, and immediate action to take appropriate precautions may be necessary. The fact that the joint report was made public raises serious concerns about the government’s ability to maintain the integrity of sensitive information intended for a limited audience. Moving forward, both the public and private sectors should take steps to ensure an effective and responsible information-sharing environment.

—Paul Tiao co-chairs Hunton & Williams LLP’s cyber and physical security task force and served as senior cybersecurity counsel to former FBI Director Robert S. Mueller. Eric Hutchins is an associate in Hunton & Williams’ government relations practice.