https://www.wsj.com/articles/should-the-government-require-companies-to-meet-cybersecurity-standards-for-critical-infrastructure-1542041617

JOURNAL REPORTS: TECHNOLOGY

Should the Government Require Companies to Meet Cybersecurity Standards for Critical Infrastructure?

Some argue that government regulation is needed to keep critical systems safe from hackers. Others say industry can do a better job on its own.

The Department of Homeland Security reported in July that Russian agents had penetrated the control rooms of electric utilities. **PHOTO:** GETTY IMAGES/ISTOCK

Nov. 12, 2018 11:53 am ET

Major U.S. cities plunged into darkness. The financial system frozen. Transportation crippled. Drinking water in short supply.

These are just a few of the ways that a successful cyberattack on critical infrastructure could wreak havoc on U.S. national security, economic stability and public health and safety.

Worries that hackers are getting closer to inflicting serious damage on the U.S. were underscored in July, when the Department of Homeland Security reported that Russian agents had penetrated the control rooms of electric utilities, where they could have caused widespread blackouts.

Against that backdrop, a debate is under way about what U.S. policy makers should do to keep critical systems safe.

Some cybersecurity experts say that while industry cooperation on things such as best practices and information sharing are helpful, keeping America's critical infrastructure safe is going to require federal and state government regulation and oversight—along with appropriate funding and incentives.

Others argue that one-size-fits-all cybersecurity regulations may do more harm than good. The best way forward, they say, is to allow companies and industries to direct security resources where they believe they are needed most.

Richard Forno, director of the graduate cybersecurity program and assistant director of the Center for Cybersecurity at the University of Maryland, Baltimore County, makes the case for government standards and oversight. Anne Hobson, a program manager with the Mercatus Center at George Mason University, argues that the development of targeted, sector-specific solutions is the better option.

YES: The industry can't do it on its own

By Richard Forno

Richard Forno **PHOTO:** MARLAYNA DEMOND

Society depends on critical infrastructures like power distribution, water supply, transportation, the internet and more to be available for use all day, every day. These systems, however, are under constant attack and many are part of a cyber environment that isn't easily secured.

While some industry sectors are better able to secure themselves than others, aged, embedded and/or proprietary hardware, and the hodgepodge ways these systems have been brought into the information age are just some of the problems that make it difficult to secure them effectively.

Industry cooperation on cybersecurity standards, best practices and information sharing are helpful in fostering stronger infrastructure security on a daily basis. However, I am less sanguine that industry can handle the realities of protecting America's critical infrastructures without some degree of federal and state government regulation and oversight—along with appropriate funding and incentives—to ensure a meaningful level of acceptable security, resilience and accountability.

Light-touch approach

Many industries tend to favor self-regulation because it helps keep government away, reduces their costs and allows them to keep any problems "inside the family" and away from public view. In this arrangement, citizens are being asked to trust them to do the right things for the right reasons. This can be problematic for public companies with a primary responsibility to

their shareholders and not the general public. The 2008 financial crisis is one example where industry self-policing failed with catastrophic results.

Since self-regulation isn't sufficient, the government needs to step in. Unfortunately, government regulation can, and frequently does, create more problems than it purports to solve. To be effective and well-received, a "light touch" regulatory approach to critical infrastructure security should be objectively informed and intelligently developed, include public accountability and provide meaningful consequences.

To develop the regulations, policy makers should rely on a wider range of experts than the usual industry voices in think tanks or trade groups. Other sectors, industries and even countries may offer helpful insights.

The result would be a set of common cybersecurity standards, perhaps based on accepted international criteria like the National Institute of Standards and Technology (NIST) Cybersecurity Framework, or the European General Data Protection Regulation, or ISO 27001, an international information-security standard. Rather than reinventing the cyber-wheel, government can draw upon this treasure trove of resources in developing an effective regulatory mechanism for a given industry sector or context. There will be no one-size-fits all resolution to this issue.

Oversight must involve more than a company simply sending a completed checklist back to regulators each year. Perhaps it is time to consider random on-site inspections by competent cybersecurity experts, as well. Failing to meet these standards during routine oversight or in the aftermath of a cyber incident must be met with stringent public accountability and financial consequences. Large fines, civil or criminal liability, and increased oversight and reporting requirements, along with the adverse publicity associated with being on the wrong side of a cyber incident, can be strong incentives to maintain compliance. Unfortunately, the mechanisms the U.S. currently has in place to punish facilities that don't appropriately secure important assets are only modestly helpful.

Sharing the burden

Industry acceptance of such regulations will depend on appropriate government financial incentives to make compliance costs more palatable. The goal is to strengthen these companies and secure their growth, not hamstring industry or penalize their profits. Since both government and industry allowed these critical-infrastructure systems to be moved into the internet age without much thought to security, the cost burden should be shared equitably.

It's a good bet that those professing the laissez-faire approach to industry regulation will be the

first to wring their hands asking, “How could this happen?” after the next crisis takes place. While cybersecurity problems are inevitable, if something is deemed a critical infrastructure for the country, it needs to be treated as such and subject to competent oversight by qualified government regulators to help reduce the costs and consequences of future incidents.

Dr. Forno is director of the graduate cybersecurity program and assistant director of the Center for Cybersecurity at the University of Maryland, Baltimore County. He can be reached at reports@wsj.com.

NO: One-size-fits-all doesn’t work

By Anne Hobson

Anne Hobson **PHOTO:** LAUREN DIECKHAUS/GEORGE MASON UNIVERSITY

In 2015, Ukraine experienced the first widespread attack on a power grid, when hackers remotely switched off substations, leaving 230,000 residents without electricity for several hours. A few years before, Iranian operatives had conducted systematic cyberattacks on U.S. banks and attempted to shut down a New York dam. More recently, the U.S. Department of Homeland Security said Russian hackers had penetrated the control rooms of U.S. electric utilities, where they could have caused blackouts.

As these incidents demonstrate, successful cyberattacks on critical infrastructure are a reality. The big question is, what should U.S. policy makers do to keep systems essential to our society safe?

One proposed solution is for the government to establish mandatory cybersecurity

requirements for all U.S. companies operating critical infrastructure, and an oversight program to ensure compliance. While well-intentioned, this approach has several flaws.

False sense of security

Critical-infrastructure facilities are diverse in functionality and purpose, so one-size-fits-all requirements are bound to be vague or outdated. Codified requirements can become inflexible in the quickly evolving technological sphere. Design standards requiring a company to use a specific encryption protocol, for example, could compromise the functionality or speed of some of these systems.

In addition, critical-infrastructure facilities aren't equally vulnerable to cyberthreats because they don't rely equally on digital technologies. As such, mandatory cybersecurity requirements could be inadequate for some sectors and needlessly onerous for others.

What's more, regulatory compliance can foster a false sense of security that blinds management to the need to invest in improved defenses against emerging vulnerabilities. Efforts spent hardening current systems can take away from the development of a newer, more resilient system as companies redirect labor and resources toward regulatory compliance.

A new set of government cybersecurity requirements would duplicate existing federal efforts to incentivize good cybersecurity practices in critical sectors. The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides cybersecurity risk-assessment guidelines and includes language on securing digital infrastructure. NIST, which is part of the U.S. Commerce Department, specifically designed the framework as a requirement for companies designated as critical infrastructure.

There also are mechanisms in place to punish facilities that don't appropriately secure important assets. The Federal Trade Commission and Consumer Financial Protection Bureau, for example, are investigating the Equifax EFX **0.53%** ▲ breach that exposed the personal information of 163 million Americans. This activity may lead to fines or other penalties.

Regulate yourself

At this point, the best way forward is for government to support an institutional environment that makes it worthwhile for companies and industries to self-regulate. Importantly, this requires that companies like Equifax bear the full cost of a data breach so that they prioritize cybersecurity. The threat of losses due to a breach is the most effective method available to encourage companies to learn from each other's experiences and to do the right thing. Insulating companies from the consequences of their actions, as exemplified by the bailouts and concessions following the 2008 financial crisis, undermines these incentives.

What makes America's network of critical infrastructure resilient in the face of cyberthreats is diversity and redundancy. Banks, internet providers and manufacturers are widely distributed across the U.S., offer distinct services and have different owners and operators, making it difficult for hackers to take down a whole sector in a single cyberattack. Companies should be allowed to further build that resilience by directing security resources where they believe they are most needed.

Policy makers can help by promoting further adoption of the NIST framework, as well as encouraging the adoption of cyber insurance in key sectors. Ultimately, policy makers should focus on fostering a policy environment such that a wide set of solutions can evolve. Allowing public and private efforts to emerge to address the changing cyberthreat landscape will encourage the development of targeted, sector-specific solutions. Rather than set new mandatory cybersecurity requirements, government should convene stakeholders and promote information-sharing about evolving threats. In this way, it can support the evolution and adoption of guidelines and best practices.

Ms. Hobson is a program manager with the Mercatus Center at George Mason University. She can be reached at reports@wsj.com.

Corrections & Amplifications

Anne Hobson is currently pursing a PhD. An earlier version of this article incorrectly referred to her as Dr. in the bio. (Nov. 12, 2018)

- **Health Care**
- **Leadership**
- **Retirement**
- **Small Business**
- **Technology**
- **Wealth Management**