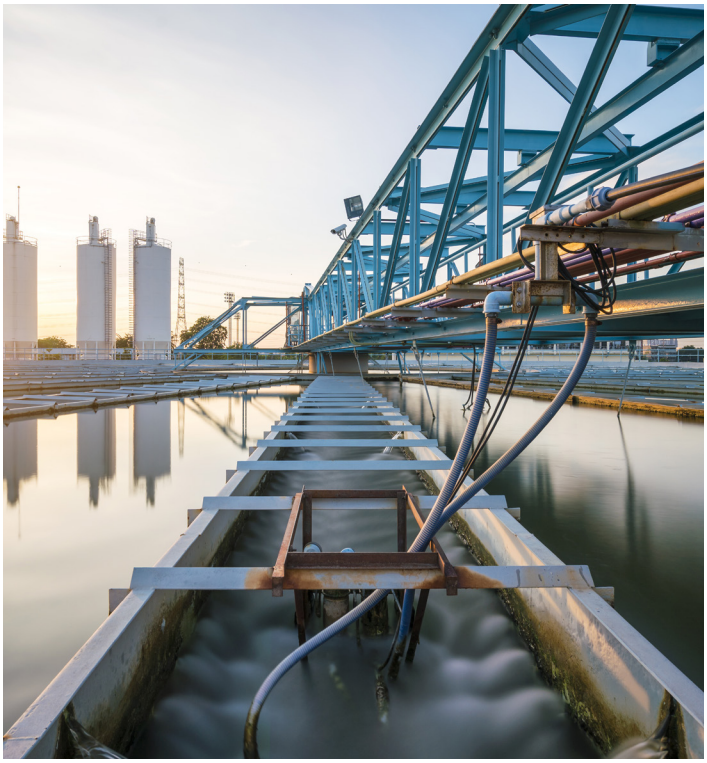
Deloitte.

Cybersecurity for critical infrastructure

Growing, high-visibility risks call for strong state leadership



In 2012, Defense Secretary Leon Panetta famously warned that the United States risked a "cyber-Pearl Harbor" with the potential for hackers to silently derail trains, release lethal chemicals, contaminate the water supply, or shut down the power grid. As adversaries change their motives and cyberattack techniques, the topic of cybersecurity is expanding far beyond citizen data protection: It is now an urgent public safety concern.

Cyberattacks on critical infrastructure have grown increasingly sophisticated—with greater potential impact.

For financial, political, or military gain, recent attacks were responsible for **shutting down Ukraine's power grid, "self-destruction" of centrifuges** in a uranium-enrichment plant in Iran, holding a Los Angeles hospital's **medical records for ransom**, and **infiltration of email and fare-collecting systems** for San Francisco public transit. To date, damages have been limited to financial loss, inconvenience, and negative publicity, but cyberattacks on critical infrastructure clearly have the potential to pose serious problems, from service disruption to physical threat to human lives.

Cybersecurity in the news

Increasingly sophisticated cyberattacks on critical infrastructure have placed governments worldwide on high alert.

Stuxnet malware targeted at industrial control systems
"Stuxnet had been specifically designed to subvert Siemens systems running centrifuges in Iran's nuclear-enrichment program ... financial gain had not been the objective. It was a politically motivated attack. ... The implications ... go beyond state-sponsored cyberattacks." David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum*, February 26, 2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

December 2015 cyberattack on Ukraine power grid
"... well planned and brilliantly executed ... it was a first-of-its-kind attack that set an ominous precedent for the safety and security of power grids everywhere ... the people in charge of the world's power supplies have been warned. This attack was relatively short-lived and benign. The next one might not be." Kim Zetter, *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid.

February 2016 ransomware attack on LA hospital
"The attack forced the hospital to return to pen and paper for its record-keeping. ... cyberattacks on hospitals have become more common in recent years as hackers pursue personal information they can use for fraud schemes." Richard Winton, "Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating," *LA Times*, February 18, 2016, http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html.

November 2016 SF public transit payment system and email hack
"Attacks like this could happen anywhere and wreak far more havoc. And they almost certainly will, because the American public transit systems that make daily life possible for millions are an easy target. Many are aging and underfunded, with barely enough money to keep the trains running, let alone invest in IT security upgrades." Jack Stewart, "SF's Transit Hack Could've Been Way Worse—And Cities Must Prepare," *Wired*, November 28, 2016, https://www.wired.com/2016/11/sfs-transit-hack-couldve-way-worse-cities-must-prepare/.

State critical infrastructure protection should address cyber threats

States have cybersecurity programs focused on citizen data protection and often separately run programs to protect critical infrastructure. Cybersecurity specifically for critical infrastructure is a missing piece that poses an increasingly urgent risk. Cyberattacks present unique challenges:

- Cyber threats lack distinct borders.
- The tactics and technologies are constantly evolving.
- Both public and private sector entities manage critical infrastructure at risk for cyberattack, requiring a coordinated effort and information-sharing processes that currently do not formally exist in many states.

As guardians of public safety, state leaders are expected to identify, protect, detect, respond, and recover swiftly and effectively from any disruption to critical infrastructure to reduce damage and restore operations and services. Currently, most critical infrastructure protection programs only address physical threats, leaving states vulnerable to cyber threats ranging from service disruption to public safety concerns. States need to expand their risk mindset to include cyber risks and lead a statewide, public-private collaboration focused on sharing information, raising awareness of roles that all groups involved should play, and establishing a unified response to cyberattacks on critical infrastructure.

Building an effective program will require time, commitment, and close cooperation between public and private entities, as well as interstate and federal agencies, including:

- Leadership support at the highest level of state government to secure funding and broad engagement; ideally, sponsored and driven by the Governor's office.
- State-led coordination of public and private entities, including developing a framework approach for guiding practices to establish open communications, leverage strengths, define roles and responsibilities, fill skills and resource gaps, and help teams work together effectively to deter, detect, and initiate an effective response to cyberattacks. This can also help identify commonalities across critical infrastructure components.

  The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) Core Elements can be leveraged as a guide for looking at the critical elements (www.nist.gov/cyberframework/csf-reference-tool).
- A state agency serving as an information-sharing engine for all entities involved and providing access to services that specifically support a strengthened cybersecurity posture for critical infrastructure.
- Ongoing cooperation between diverse, dispersed groups, including many that have not worked together in the past: IT cybersecurity specialists dedicated to individual state agencies; emergency management and law enforcement teams responsible for on-the-ground response to critical infrastructure emergencies; private sector cybersecurity and disaster response teams; and other entities responsible for securing critical infrastructure.
- Utilization and coordination with federal partners such as Department of Homeland Security (DHS) Physical Security Advisors, DHS Cybersecurity Advisors, and liaisons from cybersecurity agencies such as the National Cybersecurity and Communication Integration Center.
- A point of contact within the state tasked with contributing to existing federal databases and leveraging existing information to conduct more well-informed risk assessments on critical infrastructure in the state.

In short, every state should be actively preparing to protect critical infrastructure from cyberattack, a serious risk that will require a serious commitment of resources and leadership.

Currently, most critical infrastructure protection programs only address physical threats, leaving states vulnerable to cyber threats ranging from service disruption to public safety concerns.

New mindset for managing cyber risk to critical infrastructure

With cyberattacks on critical infrastructure of increasing concern and rising severity, states need to view hiring and training of cybersecurity resources through a new lens. In addition to technical skills, an effective program will require leaders who can encourage strong public-private collaboration and open information exchange. In particular, private sector entities should be able to share sensitive information about potential vulnerabilities around their ability to protect critical infrastructure from cyber risks without fear of reprisal or concern that the information will be made public.

New skill combinations will also be essential. Cybersecurity specialists and teams responsible for critical infrastructure will need to consult with each other and expand their skillsets to develop a complete, accurate picture of vulnerabilities, issue severity, and possible impacts. For example, to accurately reflect risk exposure and protect the power grid from cyberattack, states will need combined expertise in cyber and the cascading impacts of destabilizing the physical power stations. It is also important to consider that preventive measures are not always foolproof. Improving awareness of how new threats present themselves and being able to detect abnormal conditions and expedite responses are essential to reducing harm to the public when attackers are successful.

An effective program will require a team with the skills to establish:

- Strong relationships with private sector and federal partners
- Well-defined roles and responsibilities and consistent and informed communications
- Mechanisms to present and receive feedback, raise awareness, support information exchange, and promote action
- Cybersecurity risk analysis and prioritization in the event of a disruption of service or physical harm to citizens
- An operational plan to share and maintain cybersecurity information
- Training and coordination for multi-disciplined response teams—search and rescue, emergency medical support, IT cybersecurity specialists, as well as leaders in the public and private sectors
- Initial and ongoing requirements for equipment and software

Each state will need to assess existing resources and begin training to fill skill and information gaps.

Defining critical infrastructure

The US Department of Homeland Security defines critical infrastructure as "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[1]

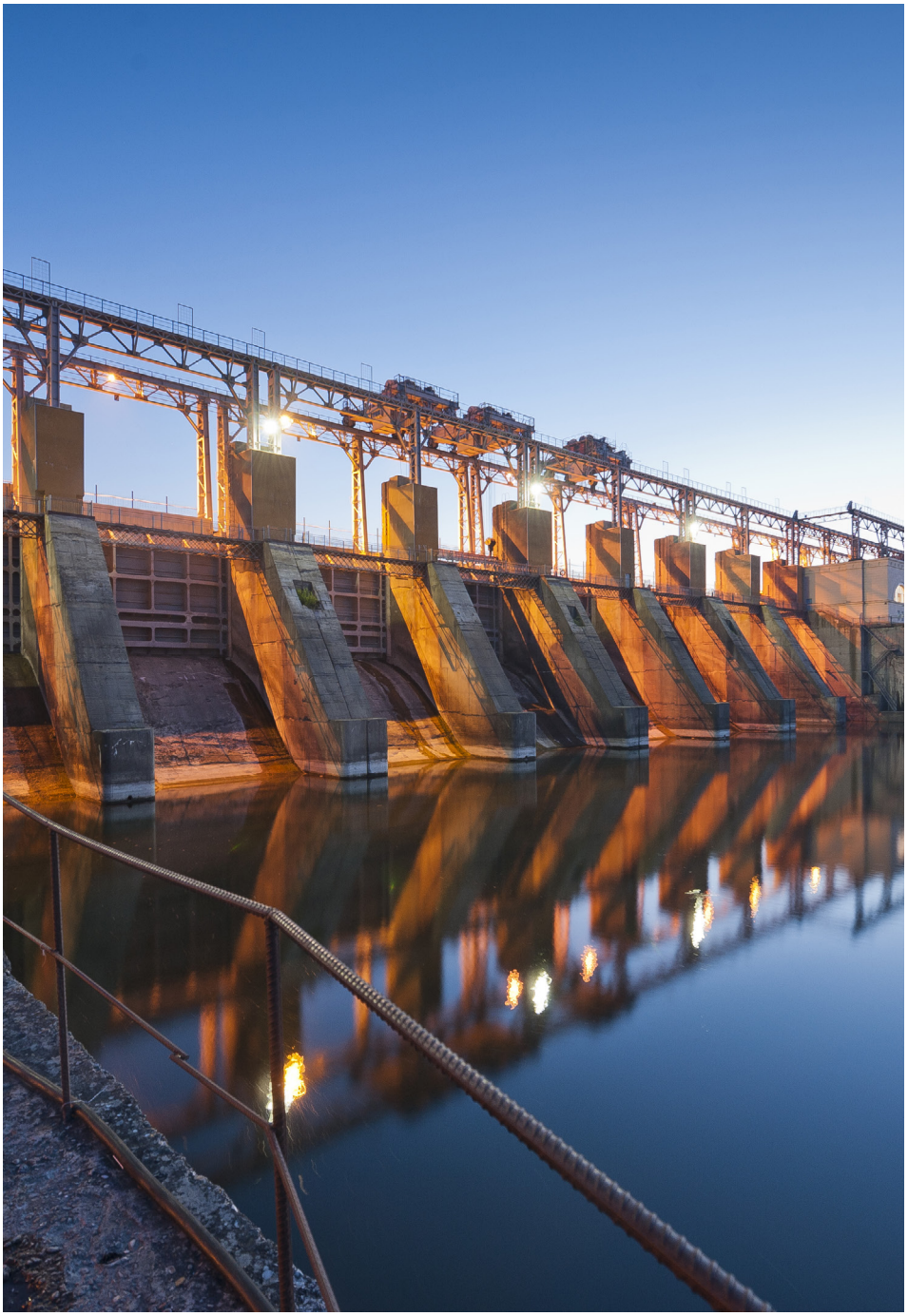
State cybersecurity programs should reflect the specific vulnerabilities of any critical infrastructure the state relies on for public health, safety, and prosperity.

Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, identifies 16 critical infrastructure sectors.[2]

Chemical	Financial services
Commercial facilities	Food and agriculture
Communications	Government facilities
Critical manufacturing	Health care, public health
Dams	Information technology
Defense industrial base	Nuclear reactors, nuclear materials and waste
Emergency services	Transportation systems
Energy	Water and wastewater systems

1. U.S. Department of Homeland Security, "*What is Critical Infrastructure?*" Last published October 14, 2016, https://www.dhs.gov/what-critical-infrastructure.
2. The White House, Presidential Policy Directive 21 (PPD-21), "*Presidential Policy Directive — Critical Infrastructure Security and Resilience*," February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Getting started: Understanding the state of your state



Building a cybersecurity critical infrastructure program takes time, careful planning, and ongoing support from the state's Governor, state and federal agencies, and public and private entities overseeing critical infrastructure. The first step is often the most difficult but it is also arguably the most important. Keeping it simple and straightforward will help accelerate the process.

The first step is helping key players in government understand the severity, urgency, and potential impacts of different types of cyber threats and the need to take immediate action. From there, the process is about assessing potential exposure. States should challenge themselves to ask the tough questions.

- Are the right people aware that this is an issue?
- Who is responsible for managing the risk?
- Do we know our attack footprint?
- What are we doing to address the issue and manage it going forward?

Once a basic understanding of potential exposure is developed, states can begin to move forward on a plan for bringing the right people and skills together to build a successful program. Maintaining focus and not losing sight of the mission will keep you on the path forward.

What next?

State leaders are best positioned to understand critical infrastructure risks within their state and develop programs to help mitigate and respond effectively to the wide variety of cyber threats they might face. However, to be successful, states will need to cultivate the skills, culture, and mindset for public-private collaboration on critical infrastructure protection programs that account for the possibility of cyber disruption.

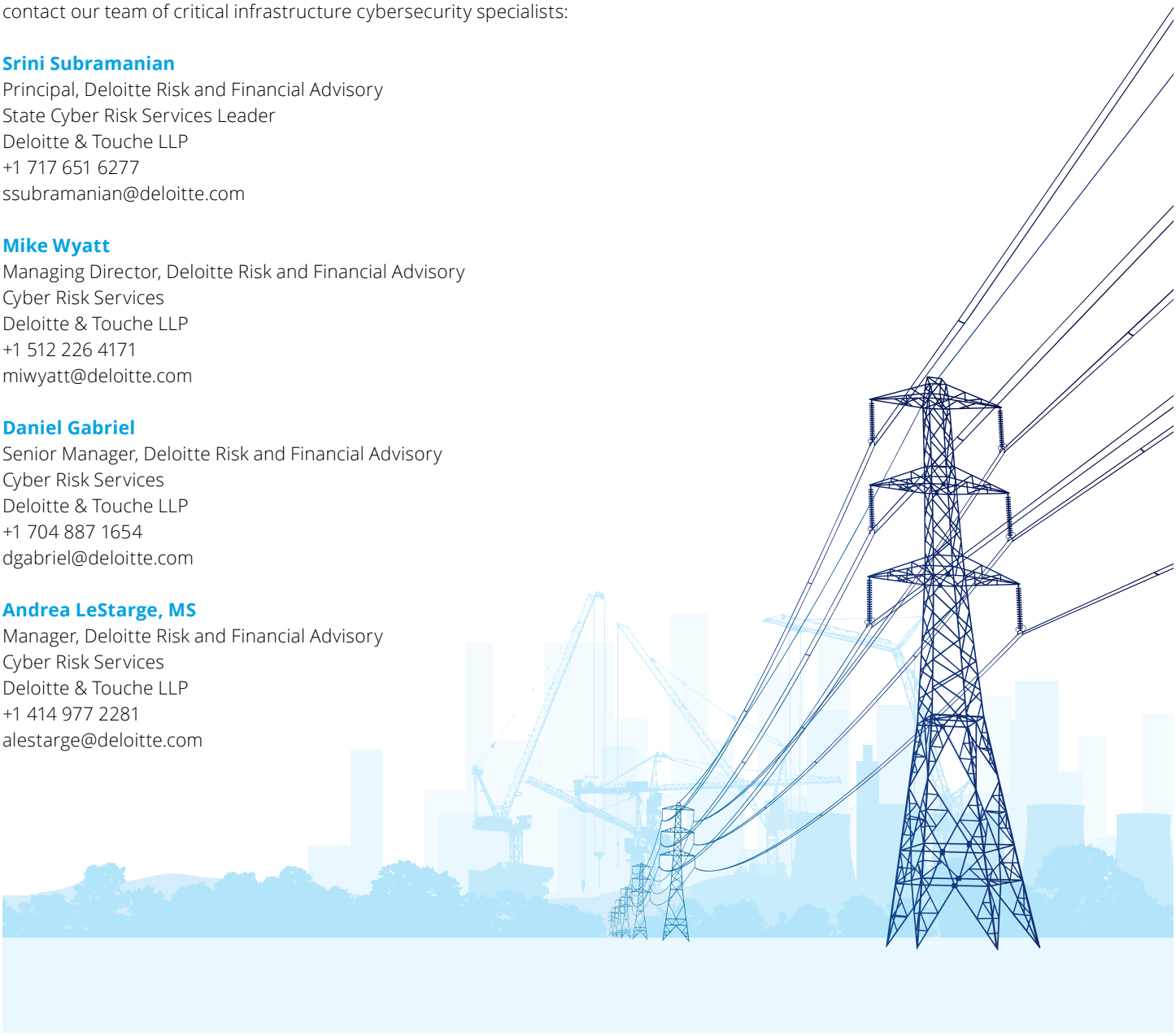
To learn more about how Deloitte can help your state evaluate options, visit our website or contact our team of critical infrastructure cybersecurity specialists:

Srini Subramanian
Principal, Deloitte Risk and Financial Advisory
State Cyber Risk Services Leader
Deloitte & Touche LLP
+1 717 651 6277
ssubramanian@deloitte.com

Mike Wyatt
Managing Director, Deloitte Risk and Financial Advisory
Cyber Risk Services
Deloitte & Touche LLP
+1 512 226 4171
miwyatt@deloitte.com

Daniel Gabriel
Senior Manager, Deloitte Risk and Financial Advisory
Cyber Risk Services
Deloitte & Touche LLP
+1 704 887 1654
dgabriel@deloitte.com

Andrea LeStarge, MS
Manager, Deloitte Risk and Financial Advisory
Cyber Risk Services
Deloitte & Touche LLP
+1 414 977 2281
alestarge@deloitte.com



Further reading

Executive order expected on cybersecurity
Jose Pagliery, "Big changes in Trump's cybersecurity executive order," *CNN*, January 31, 2017, http://money.cnn.com/2017/01/31/technology/trump-cybersecurity-executive-order/index.html.

Time Person of the Year 2016 No. 3
The Hackers. Matt Vella, "They made vulnerability the new normal and took aim at democracy itself," *Time* magazine, http://time.com/time-person-of-the-year-2016-hackers-runner-up.

Department of Homeland Security 2013 report on improving cybersecurity for critical infrastructure
www.dhs.gov/sites/default/files/publications/dhs-eo13636-analytic-report-cybersecurity-incentives-study.pdf.

National Institute of Standards and Technology (NIST) framework for improving cybersecurity for critical infrastructure
www.nist.gov/cyberframework.

White House policy on cybersecurity
www.whitehouse.gov/issues/foreign-policy/cybersecurity.

Deloitte.