

RISK-BASED V. COMPLIANCE-BASED UTILITY CYBERSECURITY — A FALSE DICHOTOMY?

Wei Chen Lin and Dominic Saebeler[*]

Synopsis: There is overwhelming consensus that energy systems are both at the heart of US critical infrastructure and increasingly in the crosshairs of escalating worldwide cybersecurity threat. The operational continuity of those critical energy systems is central to the safety and security of the United States. However, disagreement persists regarding how to best ensure those systems are sufficiently resilient against disruption from cyber-attacks. As government entities—particularly state public utility commissions—increasingly focus on cybersecurity of energy systems, questions continue to emerge as to the optimal approach to ensure cyber resiliency. Tension exists because regulators are expected to incentivize behavior by creating measurable compliance driven frameworks. Utilities, on the other hand, typically argue for a more flexible and dynamic risk-based framework focused on rapidly allocating resources to address the most important and immediate threats to energy systems.

Stakeholder conversations often frame the discussion in terms of whether a risk-based or compliance-based approach is more appropriate. Proponents of each approach typically point out the shortcomings of the other approach. For example: risk-based approaches are often characterized as variable, less structured and difficult to measure and assess. Compliance-based approaches, while considered reliable, may be static, inflexible, and quickly out of date.

Rather than categorize risk-based and compliance-based approaches as conflicting and mutually exclusive, this article proposes they be viewed as complementary (with each serving a different purpose). It also recognizes that both approaches are likely to continue in some form because of the requirement for regulatory oversight to ensure minimum levels of security are achieved, while implementing the most effective and timely overall security measures. Additionally, the article recognizes the existence of overlapping jurisdictional and organizational requirements.

Further complicating the issue, energy delivery systems are interconnected and interrelated, but cyber defense capabilities of each interconnected system are not uniform. Large systems have typically established mature and sophisticated risk-based cyber defense postures and have allocated the resources needed to assure adherence to government-required compliance-based frameworks. Smaller entities, with limited resources may struggle to match those larger systems' de-

* Wei Chen Lin is Policy Advisor in the Office of Cybersecurity and Risk Management (C&RM) at the Illinois Commerce Commission (ICC). Dominic Saebeler is the first Director of C&RM at the ICC. The views expressed represent strictly those of the authors at the time of writing and may not necessarily agree with positions of ICC Commissioners or Staff. The authors may change those views and opinions as new information becomes available. All errors are our own.

fense postures. Large-scale disruptive events often drive additional regulatory requirements increasing the burden on resources. But, experience suggests new requirements are sometimes necessary where some entities may otherwise choose to accept unreasonable risk.

Legislative reactions and overreactions, reputational damage, operational damage, and financial damage tend to cascade throughout the industry.

There is an opportunity for stakeholders to come together to solidify a path out of that chaos with a conversation to develop sensible requirements and continued partnership between government and companies in different sectors, as well as coordination between sectors. All stakeholders must respect the role and expectations of others if an integrated approach is to work.

Such an alignment could establish a multi-pronged approach that combines a minimum level of required security that protects consumers, while allowing room for critical infrastructure operators to innovate and quickly adjust to meet emerging needs. A carefully crafted combined approach could achieve the desirable qualities of both compliance-based and risk-based approaches, with one setting a floor of sensible protective measures while the other promotes flexible specific actions to rapidly improve overall security defense and response posture.

I. INTRODUCTION

There is overwhelming consensus regarding the need for continuously improving critical infrastructure security.[1] However, how we maintain an appropriate level of security remains subject to a variety of interpretations.

The crucial question is often presented in a way that seeks to select the better of the two approaches—risk-based or compliance-based.[2] Both seek to increase overall security, albeit using very different decision-making lenses.[3] Instead of selecting one approach over the other, we propose viewing these two approaches as complementary, rather than diametrically opposed to each other. The result is the retention of generally agreed upon minimum levels of security combined with the flexibility to dynamically allocate resources toward preventing the most significant risk at any given time.

The authors of this article have participated in many stakeholder conversations that frame risk-based and compliance-based approaches as conflicting and mutually exclusive. It is more likely that these different approaches will continue coexisting as both approaches seek to improve overall security, albeit in different ways, and because of overlapping jurisdictional and organizational requirements that will continue for the foreseeable future.

However, an opportunity exists for a multipronged approach to be considered that views risk-based and compliance-based approaches as complementary, with one setting a floor of assurance while the other promotes flexible specific actions that rapidly improve overall security.

Economist Alfred E. Kahn, who chaired the New York Public Service Commission from 1974–1977, is generally attributed with saying "[a]ll regulation is incentive regulation."[4] Consistent with this concept, regulators are generally expected to create measurable, compliance driven frameworks.[5] Such requirements are necessary to prevent corners from being cut by entities willing to accept certain risks regulators deem unacceptable.[6] While acknowledging the need for some level of regulation, utilities will typically also argue for the freedom to implement a more dynamic risk-based framework focused on flexible al-

---

1. *Using the Cybersecurity Framework*, DEP'T OF HOMELAND SEC. (Aug. 22, 2018), https://www.dhs.gov/using-cybersecurity-framework.

2. Robert S. Kaplan & Anette Mikes, *Managing Risks: A New Framework*, HARV. BUS. REV. (June 2012), https://hbr.org/2012/06/managing-risks-a-new-framework.

3. *Id.*

4. Inara Scott, *Incentive Regulation, New Business Models, and the Transformation of the Electric Power Industry*, 5 MICH. J. ENVTL. & ADMIN. L. 319, 320 & n.1 (2016); *see generally* Alfred E. Kahn, *Deregulation: Looking Backward and Looking Forward*, 7 YALE J. REG. 325 (1990).

5. Kahn, *supra* note 4, at 337 n.28.

6. *Id.*

location of resources toward addressing the most important and immediate emerging risk.[7]

Both approaches are designed to ensure that security protocols are consistently operating as intended, progress towards increased security is measurable, and risk is actually reduced.[8] Many security professionals are concerned that actual risk is often not reduced through many "check box" compliance steps that can quickly become obsolete as threats continuously change and mature.[9] Further, meeting compliance requirements arguably consumes money and resources that might otherwise be allocated by the company to risk-based activities, some of which might help achieve increased security by responding to evolving threats instead of legacy threats some regulations target.[10]

Many challenges exist, including proper resource allocation and timely solution implementations that relate directly to assurance activities for compliance-based frameworks, such as internal and external assessments, investigation, evaluation, self-certification, self-auditing, self-reporting/disclosure, and third-party auditing.[11] Appropriate security investments should be seamlessly integrated into the business process to achieve continuous assessment and mitigation of risks.[12] Implementing metrics that support optimal levels of investment is also critical to determining the effectiveness of cybersecurity defense measures.[13]

This article will define key concepts such as risk, threat, and vulnerability. It will then discuss how the merger of Information Technology (IT) and Operational Technology (OT) is leading to the recent increased focus on cybersecurity of energy systems. This article will also discuss the ever-increasing role of the consumer in energy resiliency due to the increasing potential for bi-directional flow of energy. Additionally, it evaluates new research on the disruptive potential of demand side cyber-attacks from coordinating malicious action of infected Internet of Things (IoT) devices that present large energy loads. Collectively, these complex and dynamic threats create a significant risk to today's modern distribution grid as well as the bulk electric system of the future.

To fully understand the complexity of establishing and implementing structured approaches to security activities, it is important to consider the various regulatory regimes, standards, frameworks guidelines, and best practices that all seek to direct utilities to increase security in a systematic and measurable manner. Multiple entities are actively engaged in advising, directing and promoting

---

7. Scott, *supra* note 4, at 346.

8. *Id.* at 337.

9. *Id.* at 335.

10. *Move To A Risk-Based Security Strategy*, CDW, https://www.cdw.com/content/dam/CDW/PDF/risk-based-security.pdf (last visited Sept. 8, 2019).

11. *See generally id.*

12. *Managing Information Security Risk: Organization, Mission, and Information System View*, COMPUT. SEC. RES. CTR. (Mar. 2011), https://csrc.nist.gov/publications/detail/sp/800-39/final.

13. *Id.*

consistent and flexible approaches to driving behavior that increases the overall security of critical infrastructure.[14]

Additional sources of direction include: The North American Electric Reliability Corporation (NERC) Reliability Standards (focusing on Critical Infrastructure Protection (CIP)),[15] Transportation Security Administration (TSA) Pipeline Security Guidelines,[16] and the International Organization for Standardization (ISO) 27000-series.[17] One specific example is the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), which is being widely adopted as it already includes compliance with applicable laws and considers compliance with regulation as one area of risks to be considered.[18] This type of broad acceptance is an example of where both risk-focused and compliance-focused structures can co-exist.

The activities of state governments, including cybersecurity legislation, rules, and orders, will be discussed and analyzed to demonstrate a context for some of the important decisions that will need to be made moving forward, especially at the distribution level, which is generally excluded from federal oversight. Finally, this article will explain why framing the compliance and risk-based approaches as two extremes is misleading and diminishes the potential value of each. The opportunity exists to align compliance activities and risk-based security practices through continued stakeholder collaboration on creative policies, flexible statutory requirements, and streamlined industry standards to reduce duplication of efforts and support streamlined investment.[19]

Such an alignment will help establish a minimum level of security to protect consumers, while also allowing critical infrastructure operators to innovate and continuously improve their security postures.[20] Incorporation of each approach in a way that maximizes their respective strengths and minimizes their weaknesses in a complementary way should be the optimal solution. The result should be achievement of an acceptable level of security across the industry at reasonable cost, while still maintaining optimal levels of security, preparedness, and resilience.[21] Ideally, that achievement should be independent of the backdrop of necessary regulation and compliance requirements.

---

14. *See generally Infrastructure Security*, DEP'T OF HOMELAND SEC. (June 17, 2019), https://www.dhs.gov/topic/critical-infrastructure-security.

15. *See generally Critical Infrastructure Protection Committee (CIPC)*, N. AM. ELEC. RELIABILITY CORP., https://www.nerc.com/comm/CIPC/Pages/default.aspx (last visited Sept. 8, 2019).

16. *See generally Pipeline Security Guidelines*, TRANSP. SEC. ADMIN. (Mar. 2018), https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf.

17. *See generally ISO/IEC 27001 Information Security Management*, ISO, https://www.iso.org/isoiec-27001-information-security.html (last visited Sept. 8, 2019).

18. *See generally Framework for Improving Critical Infrastructure Cybersecurity*, NAT'L INST. OF STANDARDS AND TECH. (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

19. *Id.*

20. *Id.* at 6.

21. *Id.* at 8, 27.

II. BACKGROUND

Utilities often advocate for a hands-off approach to cyber security oversight.[22] This article presents a combined solution that addresses the perceived dichotomy between risk-based and compliance-based approaches.

The bulk power system is subject to federal regulation through the Federal Energy Regulatory Commission (FERC) and implementation through NERC CIP Reliability Standards.[23] However, there is generally no federal jurisdiction at the distribution level,[24] resulting in a potential gap where no consistent cybersecurity approach or requirements exists across the United States.

State public utility commissions are now faced with determining if, and how much, regulation should be created at the distribution level.[25] The same risk-based versus compliance-based approach question is again presented as two diametrically opposing perspectives. Utilities continue to argue for utilizing a risk-based approach at the distribution level that is flexible and timely,[26] while state regulators typically mirror federal standards that focus on the achievement of compliance-based approaches to ensure the optimal level of oversight, and that accountability exists within their jurisdictions.[27] But the two can be viewed as complimentary, rather than oppositional, with one approach setting the floor and one building upon the floor and promoting excellence.

The difference in the attack surface of distribution systems versus that of transmission systems and generation is significant.[28] Most of the risk has traditionally existed in the latter.[29] But, the risk in the distribution system is rapidly increasing because the distribution system is where most of the interaction with new technologies occurs.[30] IoT devices, smart grid components, and other po-

---

22. *See generally* Miles Keogh & Sharon Thomas, *Cybersecurity: A primer for State Utility Regulators*, NAT'L ASS'N OF REG. UTIL. COMMISSIONERS (Jan. 2017), https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F.

23. Order No. 706, *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 Fed. Reg. 61,040 (2008) (to be codified at 18 C.F.R. pt. 40).

24. *See generally Electric Grid Cybersecurity*, CONG. RES. SERV., https://crsreports.congress.gov/product/pdf/R/R45312/2 (last updated Sept. 4, 2018).

25. *Id.*

26. Keogh, *supra* note 22.

27. *See generally Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*, ENERGY.GOV (Aug. 2016), https://www.energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf.

28. The bulk Electric System (BES), composed of generation and transmission operating at 100kV or higher, generally excludes "facilities used in the local distribution of electric energy." *Bulk Electric System Definition Reference Document*, N. AM. ELEC. RELIABILITY CORP. (Aug. 2018), https://www.nerc.com/pa/Stand/2018%20Bulk%20Electric%20System%20Definition%20Reference/BES_Reference_Doc_08_08_2018_Clean_for_Posting.pdf.; *see generally Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*, *supra* note 27.

29. *See generally Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*, supra note 28.

30. *Electric Distribution System Cybersecurity Is Critical In Today's Interconnected Society*, EDISON ELEC. INST. (Apr. 2018), www.eei.org/issuesandpolicy/Documents/EEI_cybersecurity_considerations_Distribution_Fin-April/27-2018.pdf.

tential points of entry are proliferating primarily along the distribution pathway.[31]

While transmission lines connect the backbone of the grid together and take electricity from generation to the utilities that distribute to the home, each connection point is now much more securely managed both in volume and construction as a result of lessons learned from prior large-scale blackouts.[32] Regulation of distribution security has not, until recently, been viewed as important as that of generation and transmission systems; but as distribution level risk increases, the discussion of which approach (risk or compliance) is best suited to assure utilities secure their infrastructure becomes more important.[33] This is where a hybrid approach stands the best chance of properly addressing the evolving risk because it can provide the proper incentives to utilities to maintain minimum levels of security while simultaneously encouraging flexible responses to novel threats and quick decision making.[34]

Utility operations are becoming increasingly connected or "smart."[35] The search for efficiencies has increased reliance on smart technologies and automation.[36] That reliance has increased complexity. The increased complexity, in turn, prompts additional and continuous exploration of technological options that provide increased efficiencies while the entire process repeats itself.[37]

"The crux of each 'smart grid' technology . . . is that it seeks to create a two-way communications link or channel."[38] That, in turn, creates an ever-expanding attack surface through the introduction of new threat vectors (the device or vulnerability used to attack the target),[39] at all levels of the energy sector,[40] from the plant operator's remote access to oil and gas operations,[41] to a consumer's internet connected voiced controlled microwave.[42]

---

31. *See generally* Noshina Tariq et. al., *The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey*, NCBI (Apr. 14, 2019), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6515199/.

32. EDISON ELEC. INST., *supra* note 30.

33. COMM. ON ENHANCING THE RESILIENCE OF THE NATION'S ELEC. POWER TRANSMISSION AND DISTRIBUTION SYS., NAT'L ACAD. PRESS, ENHANCING THE RESILIENCE OF THE NATION'S ELECTRICITY SYSTEM 35 (2017).

34. CONG. RES. SERV., *supra* note 24.

35. *Id.*

36. *Id.*

37. Jesse Teas et. al., *Smart Utility Meters Enhance Utility Operations*, CONSULTING SPECIFYING ENG'R (Feb. 22, 2017), https://www.csemag.com/articles/smart-utility-meters-enhance-utility-operations/.

38. Roland L. Trope & Stephen J. Humes, *Before Rolling Blackouts Begin: Briefing Boards on Cyber Attacks That Target and Degrade the Grid*, 40 WILLIAM MITCHELL L. REV. 647, 774 (2014).

39. Phil Withers, *Information Security Threat Vectors*, ISACA (Mar. 2011), https://www.isaca.org/chapters5/Virginia/Events/Documents/Past%20Pres%20201103%20Threat%20Vectors.pdf.

40. Trope, *supra* note 38, at 647, 665.

41. *Id.*; *see generally ABB Remote Monitoring and Operations Room (ARMOR)*, ABB, https://new.abb.com/oil-and-gas/service/by-service/advanced-services/armor (last visited Sept. 8, 2019).

42. Jeffrey Van Camp, *In Defense of Amazon's Alexa Microwave*, WIRED (Sept. 23, 2018), https://www.wired.com/story/rants-and-raves-defense-of-amazon-alexa-microwave/.

As distributed energy resource (DER) penetration increases, concerns increase over potential disruption to the energy DERs supply to the grid.[43] This creates the potential for supply-side disruptions should attackers take control of "smart inverters" that are connected to both the internet and the electric grid. DERs can potentially interact with the grid through both the electrical connections and the SCADA control systems connections that keep them operating in coordination with the rest of the interconnected grid.[44]

With increased IoT penetration, demand-side disruptions also become a concern. Researchers from Princeton University simulated a scenario in which attackers control a botnet composed of power-hungry devices like air conditioners, water heaters, and space heaters.[45] By coordinating the botnet of devices to turn on or off in an orchestrated fashion, the attacker could damage components on the grid by over or under loading certain parts of the distribution system in a malicious manner.[46] The results reveal that should attackers gain control over just tens of thousands of devices, the majority of the U.S. electric grid would potentially be severely impacted.[47] In a related study, researchers from Ben-Gurion University found that unauthorized control over a large number of automated commercial lawn sprinklers, as part of commercial smart irrigation systems, could empty a water tower within an hour or flood a water reservoir overnight.[48] These, and many other systems over which utilities have little control over, are becoming more and more important to the stability of the grid.

"No responsible electric industry executive or government official would say that the electric grid enjoys absolute protection from cyberattack. The threats are too varied and mutable, and the list of potential adversaries too long, for any such assurance to be credible."[49] It is not clear what approach is best to ensure such protections. Nor is it clear who should be the primary driver of those activities. The lack of standardized approaches also increases the overall complexity of the security and operational environments.[50]

---

43. *See generally Distributed Energy Resources: Technical Considerations for the Bulk Power System*, FED. ENERGY REG. COMM'N (Feb. 2018), https://www.ferc.gov/CalendarFiles/20180215112833-der-report.pdf.

44. *Id.*

45. Saleh Soltan et. al., *BlackIoT: Botnet of High Wattage Devices Can Disrupt the Power Grid*, PRINCETON U., https://www.princeton.edu/~pmittal/publications/blackiot-usenix18.pdf (last visited Sept. 8, 2019).

46. *Id.*

47. Andy Greenberg, *How Hacked Water Heaters Could Trigger Mass Blackouts*, WIRED (Aug. 13, 2018), https://www.wired.com/story/water-heaters-power-grid-hack-blackout/.

48. Martin Giles, *Hackers Could Turn Your Garden Sprinklers into a Cyber Weapon*, MIT TECH. REV. (Aug. 8, 2018), https://www.technologyreview.com/the-download/611849/hackers-could-turn-your-garden-sprinklers-into-a-cyber-weapon/.

49. Jonathan D. Schneider, *Lights Out*, 37 ENERGY L.J. 433, 440 (2016) (reviewing TED KOPPEL, LIGHTS OUT: A CYBERATTACK, A NATION UNPREPARED, SURVIVING THE AFTERMATH (2015)).

50. *Id.*

A. Energy Systems Are Essential, yet Face Evolving Threats

"In North America, public access to a resilient and reliable supply of electric power—whenever needed—is our economic foundation; it is a critical constant supporting our quality of life and the quickening pace of digital technological innovations."[51] Often touted as the most complex and largest machine ever built, the electric grid is interconnected and interdependent between the generator and the consumer at two extreme ends of the wires.[52] There is a complex system composed of a significant amount of equipment in between the two.[53] Threats to any part of the system can potentially affect the rest of the interconnected system.[54]

> Unlike operations in many other industries, the 'balancing' activities required to maintain stable operations . . . require . . . close attention to the rapid, moment-to-moment changes in the electricity demand and supply that need to be continuously balanced—whenever they tip out of balance, they must be restored within seconds to avert tripping off cascading outages.[55]

Increased connectivity and the ability to interact remotely with operational technology gives adversaries additional opportunities to disrupt this delicate and continuous balancing act.[56] "An adversary planning a coordinated cyber-attack . . . might attempt to disrupt, disorient, and mislead such real-time responses."[57] One way to achieve this is by disrupting the control systems and manipulating the information flow between the operator and the operational systems.[58]

> If operators receive false information about equipment or system status (or information maliciously delayed to deprive it of its real-time accuracy and insight as needed for situational awareness), they may fail to react in time (as happened during the Stuxnet attack) or they could be fed data to cause them to take the wrong--and thus damaging--corrective action (e.g., shedding electric loads when digital readouts indicate erroneously--at the direction of malware--that demand is slumping when it is, in fact, surging).[59]

In January 2019, the Director of National Intelligence, Daniel R. Coats, submitted the Worldwide Threat Assessment to the Senate Select Committee on Intelligence.[60] The Assessment identified China, Iran, North Korea, and Russia

---

51. Trope, *supra* note 38, at 654.

52. *See generally The Emerging Interdependence of the Electric Power Grid & Information and Communication Technology*, PAC. NW. NAT'L LAB. (Aug. 2015), https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-24643.pdf.

53. *Id.*

54. *Id.*

55. Trope, *supra* note 38, at 678.

56. *Id.* at 680.

57. *Id.*

58. *Id.*

59. *Id.*

60. *Worldwide Threat Assessment of the U.S. Intelligence Community: Hearing Before the Senate Select Committee on Intelligence*, 115th Cong. 2 (2019) (Statement of Daniel R. Coats, Director of National Intelligence).

as increasingly using cyber operations to target critical infrastructure.[61] "In the last decade, our adversaries and strategic competitors have developed and experimented with a growing capability to shape and alter the information and systems on which we rely."[62] The report states that "China has the ability to launch cyber attacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States."[63] In addition, "Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016"[64] and that "Moscow is mapping our critical infrastructure with the long-term goal of being able to cause substantial damage."[65]

It is important to take these risks seriously, but not be paralyzed by fear. Cascading blackouts have occurred in the United States, such as the Northeast blackout of 2003[66] and the Southeastern blackout of 2011.[67] In both cases the disruptions were attributed to a series of failures in different parts of the grid.[68] Neither was the result of a cyber attack or lapse in cyber protections.[69] But like cyber events, lessons were learned, and controls put in place to prevent a repeat of these events.[70]

The United States has not yet had a reported blackout due to a cyber attack. Other countries have not been so lucky. In 2015, a cyber attack against Ukraine's distribution utilities resulted in outages for 225,000 customers across three regional electric power distribution companies' territories.[71] In that case, operators reverted to manual controls and recovered operations within hours. However, with the level of automation in the U.S. electric grid such a quick response may not be possible. Reverting to completely manual operations may not be a viable option for many segments of the grid.

---

61. *Id.* at 5.

62. *Id.*

63. *Id.*

64. *Id.* at 6.

65. *Worldwide Threat Assessment of the U.S. Intelligence Community: Hearing Before the Senate Select Committee on Intelligence*, 115th Cong. 6 (2019) (Statement of Daniel R. Coats, Director of National Intelligence).

66. *U.S./Canada Power Outage Task Force: August 14, 2003 Outage Sequence of Events*, FED. ENERGY REG. COMM'N 2 (Sept. 12, 2003), https://www.ferc.gov/industries/electric/indus-act/reliability/blackout/09-12-03-blackout-sum.pdf.

67. *Arizona-Southern California Outages on September 8, 2011*, FED. ENERGY REG. COMM'N & N. AM. ELEC. RELIABILITY CORP. 1 (Apr. 2012), https://www.ferc.gov/legal/staff-reports/04-27-2012-ferc-nerc-report.pdf.

68. *Id.* at 5; FED. ENERGY REG. COMM'N, *supra* note 66, at 14.

69. *See generally* FED. ENERGY REG. COMM'N, *supra* note 66; FED. ENERGY REG. COMM'N & N. AM. ELEC. RELIABILITY CORP., *supra* note 67.

70. FED. ENERGY REG. COMM'N & N. AM. ELEC. RELIABILITY CORP., *supra* note 67, at 11.

71. *Cyber-Attack Against Ukrainian Critical Infrastructure*, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (last updated Aug. 23, 2018).

While there are doubts that wide spread long-term blackouts could be caused by cyberattacks, few dispute that a *successful* attack would be an existential threat. There are a variety of reports on the expected impact of a prolonged disruption to the grid. Estimates for fatalities across the United States of a one-year power outage "range from two-thirds to [90%] of the population."[72] Regulators must be careful not to let the gravity of the situation overwhelm or lull them into inaction. Harmoniously leveraging both risk-based and compliance-based approaches to efficiently improve utility security is possible and important. Through leveraging risk-based and compliance-based approaches, regulatory and industry collaboration will improve reliability, resiliency, and security of energy delivery networks.

B. Risk-Based and Compliance-Based Security

Regulatory compliance is a familiar term to many. Typically, governments and standards groups set benchmarks and requirements, and organizations comply with such mandates. For investor-owned utilities, regulatory oversight is part of the regulatory compact.[73] Noncompliance with federal or state commission rules is typically accompanied by fines and penalties.

In this environment, security professionals have advocated for a shift to risk-based approaches for many years.[74] There are some basic risk management concepts that are important for regulators to understand. Many sources discuss the relative merits of risk-based and compliance-based approaches to security in depth.[75] The following are brief introductions to these basic concepts as a backdrop for the discussion of harmonizing both approaches.

1. Risk Formula and Risk Management

Risk-based approaches rely on a risk formula as a way to conceptualize risk. There are various formulations in use.

---

72. Brien J. Sheahan et al., *Vulnerability of SCADA Systems Underscore Urgent Need to Secure Utility Supply Chains*, PUB. UTIL. FORT. (Apr. 2019), https://www.fortnightly.com/fortnightly/2019/04/vulnerability-scada-systems-underscore-urgent-need-secure-utility-supply-chains?authkey=878b4c75002af87f331e4b0bda104cf6cb6ebef5163e1ad1af423f347d3ab070.

73. JIM LAZAR, ELECTRICITY REGULATION IN THE US: A GUIDE 6 (2d ed. 2016) (noting that, under the regulatory compact, utility companies are granted a protected monopoly over a service territory and operate, according to performance standards set by regulators, at a regulated price that covers operating costs and a return on investments).

74. *See, e.g.*, *NERC Full Notice of Penalty Regarding FERC Docket No. NP19-4-000*, N. AM. ELEC. RELIABILITY CORP. (Jan. 25, 2019), https://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Public_FinalFiled_NOP_NOC-2605_Part%201.pdf; Rebecca Smith, *Duke Energy Broke Rules Designed to Keep Electric Grid Safe*, WALL ST. J. (Feb. 1, 2019), https://www.wsj.com/articles/duke-energy-broke-rules-designed-to-keep-electric-grid-safe-11549056238.

75. *See, e.g.*, *NERC Full Notice of Penalty Regarding FERC Docket No. NP19-4-000*, N. AM. ELEC. RELIABILITY CORP. (Jan. 25, 2019), https://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Public_FinalFiled_NOP_NOC-2605_Part%201.pdf.

Examples include:

(1) Risk = Threat x Vulnerability x Consequence;[76]
(2) Risk = Likelihood x Impact;[77]
(3) Criticality = Probability x Severity;[78] or
(4) Risk $= \frac{\text{Probability} \times \text{Impact}}{\text{Controls}}$.[79]

The specific formulation is, for our purposes, less important than the shared elements.

Threat is the source, and the things that "use" vulnerabilities.[80] Vulnerabilities are the weaknesses, which can often be controlled.[81] Consequences are self-explanatory, and can include reputational, financial, and productivity damages that organizations do not want to incur.[82]

To calculate risk, the potential impact of an event is multiplied by the probability of that event occurring.[83] The result can be divided by the effects of available controls or compared with the cost of those controls.[84]

The term controls refers to the means by which an organization can mitigate the undesirable effects of a vulnerability being exploited, i.e., manage the risk.[85] Risk management involves the prioritization and mitigation of risks based on a balance of the costs of the undesirable effects and the costs of addressing the risk.[86] Well-accepted risk management actions include: (1) risk acceptance, an explicit or implicit decision to not directly address the risk and assume the consequences; (2) risk avoidance, by not participating in the risky activity, such as not purchasing the business or asset, or getting out of a line of business altogether; (3) risk reduction or control, by deliberately taking action to reduce a risk's

76. Koen Van Impe, *Simplifying Risk Management*, SEC. INTELLIGENCE (Mar. 28, 2017), https://securityintelligence.com/simplifying-risk-management/.

77. *Id.*

78. Frank Montgomery & Olivia Lake, *Case Study 1: Risk Assessment and Lifecycle Management Learning*, PARENTERAL DRUG ASS'N, 46 (Jan. 28, 2014), https://www.ema.europa.eu/en/documents/presentation/presentation-case-study-1-risk-assessment-lifecycle-management-learning_en.pdf.

79. Ron Woerner, *The Real Information Security Risk Equation*, TECH MARKET (Apr. 30, 2010), https://searchsecurity.techtarget.com/magazineContent/The-real-information-security-risk-equation.

80. Daniel Miessler, *The Difference Between Threats, Threat Actors, Vulnerabilities, and Risks*, DANIEL MIESSLER BLOG (Aug. 2, 2019), https://danielmiessler.com/study/threats-vulnerabilities-risks/.

81. *Id.*

82. JOHN MOTEFF, CONGRESSIONAL RESEARCH SERV., RISK MANAGEMENT AND CRITICAL INFRASTRUCTURE PROTECTION: ASSESSING, INTEGRATING, AND MANAGING THREATS, VULNERABILITIES AND CONSEQUENCES 5 (Feb. 4, 2005).

83. Jim Kent, *Risk = Likelihood x Impact*, CIO (Aug. 23, 2016), https://www.cio.com/article/3111304/risk-likelihood-x-impact.html.

84. *Id.*

85. Will Kenton, *Risk Control*, INVESTOPEDIA (Aug. 12, 2019), https://www.investopedia.com/terms/r/risk-control.asp.

86. Tom Walsh, *Security Risk Analysis and Management: An Overview*, AHIMA, (Nov. 2013), https://library.ahima.org/PB/SecurityRiskAnalysis#.XW6LHpNKgWo.

potential harm or maintain the risk at an acceptable level; and (4) risk transfer, by shifting some or all of the risk to another entity, such as insurance or contracting for indemnification.[87]

2. Perceived Relative Advantages of Risk-Based Approach

Risk-based approaches are often touted as being better suited to address the evolving threat landscape.[88] "Given the dynamic nature of cyber threats, we should ask ourselves whether mandatory reliability standards . . . can get past the uncertainty created by cumbersome procedures and regulatory delays to provide an effective means of addressing the cyber security threat to the bulk power system."[89]

Inherently, one gains flexibility as a central component of the risk-based approach, which is contrasted to an arguably rigid set of requirements that make up compliance-based approaches. This flexibility is one of the primary desired properties of risk-based approaches.[90] Instead of inevitable delays in regulation and compliance-based approaches that are slow to react to the latest threats after an incident, defenders can change their approaches on the fly to deal with emerging risks in the moment they are identified or ideally predicted through real time analysis.[91] In other words, the speed at which defenders can adapt to new threats is potentially greater under a risk-based approach.

Specificity is another perceived advantage. Regulations can be blunt instruments whereas, under a risk-based approach, defenders can fine-tune and adjust implementations to best suit the specific environment, as well as other broader considerations.[92]

3. Perceived Relative Advantages of Compliance-Based Approach

In spite of these perceived faults, regulatory compliance-based approaches have certain advantages that have resulted in their continued use. The ability to directly audit utility compliance with set rules provides a lens through which regulators are able to assess and refocus utility behavior by, for example, adjusting rules or engaging in enforcement actions.[93]

Unless particularly onerous regulations actually interfere with the ability to deliver more secure operations, they serve a useful purpose.[94] The ability to prove that a utility is actually doing measurable things that experts deem advisa-

87. *Risk Management Fundamentals*, DEP'T OF HOMELAND SEC. (Apr. 2011), https://www.dhs.gov/xlibrary/ assets/rma-risk-management-fundamentals.pdf.

88. Elizabeth M. Brereton, *Cyber Security are Four-Letter Words Enough?*, 153 No. 10 PUB. UTIL. FORT. 38, 39 (2015).

89. *Id.*

90. *Id.*

91. *Id.*

92. Neil Jeans, *Risk-Based Approach to KYC*, THOMSON REUTERS BLOG (June 14, 2016), https://blogs.thomsonreuters.com/answerson/kyc-risk-based-approach/.

93. *Id.*

94. *Id.*

ble to improve overall security—is a benefit to both the utility and the regulator.[95] Regulators can demonstrate effective oversight while utilities can demonstrate appropriate behavior through the same measurement.[96] Of course, it is more difficult to measure the effectiveness of a risk-based approach that lacks metrics because of the variability in actions and the difficulty of linking those actions to some measure tied to risk avoidance in a way that all sides can agree.[97]

In a risk-based only environment, for a regulator to ensure appropriate security controls are in place, that regulator must replicate the work done by the entity subject to review in evaluating the risks and risk management options, essentially duplicating the efforts.[98] By contrast, the uniformity created by compliance-based approaches leads to simplification of enforcement as well as economies of scale, as activities and information applicable to one entity may be widely applicable to others.[99]

C. Jurisdictional Issues

"The electric grid is a web comprised of infrastructure, devices and operating systems that are designed to interact seamlessly with one another."[100] However, there is no overarching, mandatory, comprehensive cyber protection requirements on the countless entities that operate this system, let alone the other sectors that the electric grid relies upon to operate.[101] "Significant gaps were presented by a risk-based identification system."[102] By their very nature risk-based approaches identify only the "high-risk" systems, often according to operational information available to a single entity, and "system-wide risks posed by lower-voltage systems . . . largely fell outside the scope."[103] "When the costs to protect the company from an attack outweigh the costs to recover from an attack, companies are typically willing to accept the risks rather than invest in protecting against them."[104] This presents jurisdictional and practical concerns for ensuring the continuous cybersecurity of electric grid components operated by all the interconnected entities.[105]

There are several jurisdictional issues concerning the electric grid. Regulatory authority over the Bulk Power System (BPS), involving sales for resale in

95. Brereton, *supra* note 88.

96. *Id.*

97. *Id.*

98. *Id.*

99. *Id.*

100. Brereton, *supra* note 88.

101. *Id.*

102. *Id.*

103. *Id.*

104. Chris Laughlin, Note, *Cybersecurity in Critical Infrastructure Sectors: A Proactive Approach to Ensure Inevitable Laws and Regulations are Effective*, 14 COLO. TECH. L.J. 345, 357–358 (2016).

105. NAT'L RES. COUNCIL OF THE NAT'L ACADS., TERRORISM AND THE ELECTRIC POWER DELIVERY SYSTEM 21, 44 (Nat'l Acads. Press 2012).

interstate commerce, is generally regulated by FERC.[106] However, FERC does not draft mandatory reliability standards itself.[107] Instead, the North American Electric Reliability Corporation (NERC) is responsible for the development of those standards by coordinating with industry experts, and the standards become effective upon approval from FERC.[108] The time lag between the identification of an issue and the introduction of a FERC approved compliance-based solution can be lengthy.[109]

Investor-owned local distribution systems, which primarily involve intra-state commerce and retail services, are generally regulated by state public utility commissions (PUCs).[110] However, municipal and cooperative utilities are typically not subject to the same level of PUC oversight.[111] In most states, "municipal utilities and public power districts are not subject to any economic regulation by the [PUC]," though "they are still subject to [some] regulation by statute."[112] "In about 20 states, cooperatives are subject to some form of state regulation."[113] "In some states, [PUCs] also regulate consumer-owned (i.e., cooperative and municipal) utilities, but in most states this is left to local governmental bodies and elected utility boards."[114] In addition, any utility, whether investor-owned or consumer-owned, may operate some facilities subject to some FERC regulations because they are deemed part of the BPS.[115]

As it relates to cyber attacks, some argue the jurisdiction issues are even more complicated. "Federal government responsibility for national defense concerning tangible, visible weapon attacks against tangible, visible targets is clear and familiar. But what happens when the foreign attacker launches invisible, intangible sorties . . . through the Internet . . . and eventually succeeds in making a kinetic attack?"[116] The appropriate jurisdictional boundaries are not clear because "[e]ven though the result might be long-term damage to operational

---

106. Lawrence R. Greenfield, *An Overview of the Federal Energy Regulatory Commission and Federal Regulation of Public Utilities*, FED. ENERGY REG. COMM'N (June 2018), https://www.ferc.gov/about/ferc-does/ferc101.pdf.

107. Richard Burt, *Risk-Based NERC Compliance: Assessing Risk to Bulk Power System Generation*, POWER MAGAZINE (June 1, 2016), https://www.powermag.com/risk-based-nerc-compliance-assessing-risk-bulk-power-system-generation/.

108. *Id.*

109. *Mandatory Reliability Standards for Critical Infrastructure Protection*, 122 F.E.R.C. ¶ 61,040 at P 77 (2008).

110. *An Overview of PUCs for State Environment and Energy Officials*, EPA (May 20, 2010), https://www.epa.gov/sites/production/files/2016-03/documents/background_paper.pdf.

111. *Id.*

112. LAZAR, s*upra* note 73, at 29-30.

113. *Id.* at 30.

114. *Id.* at 15.

115. *Energy Policy Act of 2005 Fact Sheet*, FED. ENERGY REG. COMM'N (Aug. 8, 2006), https://www.ferc.gov/legal/fed-sta/epact-fact-sheet.pdf.

116. Trope, *supra* note 38, at 659–60. *But see* Kate Fazzini, *Israel Says It Bombed Hamas Compound that Committed Cyberattacks*, CNBC (May 6, 2019), https://www.cnbc.com/2019/05/06/israel-conflict-live-response-to-a-cyberattack-will-lead-to-a-shift.html.

equipment and reduces, for months, the service capabilities of a critical infrastructure company (such as power plants or the transmission system), it is unclear whether the federal government or private industry has primary responsibility for addressing the incident."[117] While cyber-based attacks on the grid can implicate national security, *authority to respond to such attacks* might not be clearly delineated between federal, state, and private entities.[118]

Recent court decisions suggest the proliferation of energy storage, demand response, and distributed generation has potentially permitted FERC to blur the lines that separate federal and state jurisdictions, as well as public and private functions.[119] According to one commentator, the complex functional effects attributed to increasingly variable parts of the grid have raised further concerns over reliability and resiliency and those "lines are quickly blurring with no sign of clarity in the future."[120]

"As in most state-regulated systems, fifty jurisdictions result in a wide disparity in distribution standards. This is complicated even further by municipal electric utilities and/or electric cooperative utilities that may also operate within a state and 'are generally, but not always, exempt from state commission regulatory authority.'"[121] The result is the potential for overlaps and gaps between federal, state, local, and public/private jurisdiction. "Although largely lurking in the background, regulation over reliability of the grid may become the next jurisdictional battlefield."[122] While some disparity among the states is expected, regulators and industry should seek to collaboratively develop an approach to minimize potential conflicts rather than wait for the battlefield to emerge.

1. Existing Approaches: Federal

Moving to a uniform approach is a significant challenge as "[t]here is currently no federal cybersecurity legislation that generally applies to the energy industry" but "many believe that federal legislation is inevitable and necessary."[123] However, there exists a number of overlapping statues, regulations, and standards ranging from voluntary to mandatory.[124] For example,

---

117. *Id.*

118. *Id.* ("In other words, what if, instead of a few trees touching power lines in Ohio and tripping off the regional power grid in the Northeast, a rogue foreign actor infiltrates the power grid and trips off the same cascading outages? The attack poses an immediate and substantial danger to the nation. For that reason, it too implicates national security; but, efforts to respond to such attacks on the defense and information technology sectors of critical infrastructure (and they have occurred) have not been well organized, coherent, vigorous, or particularly effective.").

119. Amy L. Stein, *Reconsidering Regulatory Uncertainty: Making a Case for Energy Storage*, 41 FLA. ST. U. L. REV. 697 (2014).

120. Amy L. Stein, *Regulating Reliability*, 54 HOUS. L. REV. 1191, 1195 (2017).

121. *Id.* at 1213.

122. *Id.* at 1196.

123. Roberta D. Anderson et al., *Proceedings of the 36th Annual Institute, Chapter 28. Cybersecurity in the Era of Unconventional Development: Is the Energy Sector Ready for Cyber Attacks?*, 36 E. MIN. L. FOUND. § 28.02 (2015).

124. *Id.*

NERC, as directed by FERC, promulgates standards for the bulk electric systems.[125] The Nuclear Regulatory Commission (NRC), promulgates standards for nuclear power plants.[126] The Department of Homeland Security (DHS) promulgates the Chemical Facility Anti-Terrorism Standards (CFATS)[127] and the Transportation Security Administration (TSA) promulgates the Pipeline Security Guidelines.[128] The Department of Energy (DOE) has published the Electricity Subsector – Cybersecurity Capability Maturity Model (C2M2)[129] as well as the Oil and Natural Gas C2M2 (ONG-C2M2).[130] In addition, the Federal Communications Commission (FCC) has a history of regulations for telecom-specific companies.[131]

The present regulatory regime presents gaps and risks.[132] Protecting power systems is complicated by the evolving threat, heterogenous systems, and jurisdictional challenges.[133]

> It is not simply a matter of managing the negative externalities of an industrial process to guard against a foreseeable risk to public safety. . . . Standards also must remain flexible enough to accommodate a diverse network of systems and devices deployed across thousands of miles of infrastructure shared and owned by a diverse collection of public and private enterprises.[134]

NERC CIP generally only applies to the bulk power system, "comprising the largest generators and high-voltage transmission assets," and specifically excludes much of the distribution systems.[135] These distribution systems are squarely in the purview of state PUCs who ensure the safety and reliability of these systems, which now inevitably involves cybersecurity matters.[136]

2. Existing Approaches: States

Many state PUCs have responded to public reports of nation-state actors attacking utility operations.[137]

> Cybersecurity is a new operational element for PUCs to regulate. And it's particularly challenging because, unlike forecasting load, acquiring resources, or rate set-

125. *Id.*

126. *Id.*

127. *Id.*

128. *Pipeline Security Guidelines*, TSA (Mar. 2018), https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf; Michael Brooks, *TSA Defends Pipeline Security Practices Before FERC*, RTO INSIDER (Apr. 1, 2019), https://www.rtoinsider.com/tsa-pipeline-security-practices-ferc-113836/.

129. Anderson, *supra* note 123.

130. Hillary Hellmann, *Acknowledging the Threat: Securing United States Pipeline Scada Systems*, 36 ENERGY L.J. 157, 173 (2015).

131. *Wireless Telecomm.*, FED. COMMC'NS COMM'N, https://www.fcc.gov/wireless-telecommunications (last visited Sept. 1, 2019).

132. Brereton, *supra* note 88, at 39.

133. *Id.*

134. *Id.*

135. Andy Bochman, *Cybersecurity and the PUC*, 152 No. 4 PUB. UTIL. FORT. 26, 27 (2014).

136. *Id.*

137. *Id.* at 28.

> ting, the cybersecurity posture of a utility system can change daily, if not more frequently. Although it seems simple enough for utilities to employ cyber-security experts, the same doesn't apply to most PUCs. In order to prevent cyber-security threats — and to adapt and respond to them — a utility needs a certain level of flexibility to take fast action. Where such actions require PUC oversight or approval, the utility might need quick turnaround.[138]

The tension between the need for accountability and flexibility have led to states taking differing approaches to address the perceived problem.[139] As a result, many state PUCs are actively engaged in assessing and interpreting the prudency of the threat postures of utilities operating within their respective states.[140] Initially, those concerns have focused on the distribution systems as

> federal reliability standards have traditionally ended at the edge of the bulk energy grid, leaving states to regulate reliability as they see fit within their exclusive distribution sphere. As a result, state regulation of reliability is varied, with some states declining to mandate reliability standards at all. Reliability standards follow these bright lines, and their respective impacts are largely contained within these separate jurisdictional boxes.[141]

In August 2018, the NARUC Staff Subcommittee on Critical Infrastructure released a survey to participating members focusing on PUC strategy and activity regarding cybersecurity.[142] The authors had the opportunity to interpret the resulting data after assisting with the design of the questions, as well as the collection, compilation, and processing of the survey data.[143] The detailed results, expected by the summer of 2019, show state PUCs are taking a wide range of approaches to the problem, with differences in maturity, formality, and risk-based versus compliance-based approaches.[144] Some states are directing utilities to provide formal written responses to a set of questions while other states are meeting with utilities and having discussions about approaches, best practice adoption and how utilities are measuring their ability to increase security and respond to growing threat vectors.[145] Some states have imposed limited mandatory cybersecurity requirements.[146]

> In short, both physical and cyber-attacks on one component of the electric grid have impacts beyond the jurisdictional boundaries [of FERC]. While attacks on critical transmission infrastructure are likely to have far-reaching ripple effects on the dis-

---

138. *Id.* at 27.

139. Stein, *supra* note 120, at 1195.

140. *Id.* at 1254.

141. *Id.* at 1193–1194.

142. Peter Behr, *Util.: Researchers Tackle Wide Gap in States' Cyberdefenses*, ENV'T & ENERGY PUB. (Feb. 11, 2019), https://www.eenews.net/stories/1060120153; Lynn P. Costantini & Matthew Acho, *Understanding Cybersecurity Preparedness: Questions for Util.*, NAT'L ASS'N OF REGULATORY UTIL. COMM'RS (June 26, 2019), https://pubs.naruc.org/pub/3BACB84B-AA8A-0191-61FB-E9546E77F220.

143. Costantini, *supra* note 142.

144. *Cybersecurity Strategy Development Guide*, NAT'L ASS'N REG. UTIL. COMM'RS (Oct. 30, 2018), https://pubs.naruc.org/pub/8C1D5CDD-A2C8-DA11-6DF8-FCC89B5A3204.

145. *See id.*

146. *See id.*

> tribution grid, attacks on the distribution grid have the potential to impact the overall reliability of the entire system.[147]

The following are brief examples of how certain states have engaged with utilities to assess security efforts. While this is not an exhaustive list of state activities, it provides some interesting context and examples of how states are approaching cyber related threats.[148]

a. Florida

Since 2014, the Florida Public Service Commission (FPSC) Office of Auditing and Performance Analysis has conducted periodic reviews of the physical and cyber security measures in place for transmission and distribution assets not subject to the mandatory NERC standards at the four (4) largest Florida electric Investor-Owned Utilities' (IOUs) jurisdiction.[149] The reports also document the utilities' interactions with other governmental and industry organizations.[150] Reports are available on the FPSC website.[151]

b. Michigan

In December 2018, the Michigan Public Service Commission (MPSC) approved revisions to its rules on Electrical Technical Standards requiring IOUs and cooperative utilities to provide annual and incident reporting to the MPSC.[152] That same month the MPSC completed an Issue Brief addressing their actions on cybersecurity.[153] The MPSC is also exploring cybersecurity standards for gas distribution facilities while considering the newly updated American Petroleum Institute (API) Standard 1164 on SCADA security.[154]

c. New Jersey

In 2016, New Jersey issued the Board of Public Utilities (BPU) Cybersecurity Order,[155] mandating utilities comply with its comprehensive utility cyber se-

---

147. Stein, *supra* note 120, at 1234–35.

148. For additional details, reference the NARUC report once published. NAT'L ASS'N REG. UTIL. COMM'RS, *supra* note 144.

149. *Review of Cyber & Physical Security Prot. of Util. Substations & Control Ctrs.*, FLA. PUB. SERV. COMM'N OFFICE OF AUDITING & PERFORMANCE ANALYSIS (Apr. 2018), http://www.floridapsc.com/Files/PDF/Publications/Reports/General/Electricgas/Cyber_Physical_Security.pdf#search=security.

150. *Id.* at 3.

151. *Id.* at 65.

152. News Release, *MPSC Adopts Gas Safety, Util. Cybersecurity, Telecom Rules*, MICH. PUB. SERV. COMM'N (Dec. 20, 2018), https://mi-psc.force.com/sfc/servlet.shepherd/version/download/068t0000003HVmlAAG; *see also*, *To Promulgate Rules Governing Gas Pipeline Safety*, No. U-17826, 2018 WL 6829759, at 9 (Mich. Pub. Serv. Comm'n. Dec. 20, 2018), https://mi-psc.force.com/sfc/servlet.shepherd/version/download/ 068t0000003HSGLAA4 (providing review of regulations changed).

153. *Issue Brief: Cybersecurity*, MICH. PUB. SERV. COMM'N (Dec. 20, 2018), https://www.michigan.gov/documents/mpsc/Cybersecurity_Issue_Brief_121918_FINAL_641503_7.pdf.

154. *Michigan Statewide Energy Assessment—Initial Report*, MICH. PUB. SERV. COMM'N (July 1, 2019), https://www.michigan.gov/documents/mpsc/Sea_Initial_Report_with_Appendices_070119_659452_7.pdf.

155. *In re Util. Cyber Security Program Requirements*, 328 P.U.R.4th 169 (N.J. P.U.C. Mar. 18, 2016).

curity program requirements, including cybersecurity risk management (identify, analyze, control, monitor), maintain situational awareness, incident reporting, response and recovery, and security awareness training.[156] Appropriate executive-level personnel at each utility with authority for the utility's cybersecurity program must certify compliance with the order and associated program requirements by submitting a certificate of compliance each year.[157]

d. New York

New York has extensive experience dealing with cyber and homeland security issues. This section discusses a recent example of New York activity with respect to the financial services sector. Though not directly related to the utility sector, New York's actions are useful to understand the regulatory reaction that can occur after a high-profile incident in a critical infrastructure sector. It also shows how states can encourage an industry to adopt certain security focused behavior that it may not have adopted. The initial design of these regulations and the subsequent recommendation by the federal government for prompt adoption among the states could be informative to the utilities industry. The New York Department of Financial Services (NYDFS) supervises many financial institutions licensed to do business in the state of New York, including banks and credit unions, check cashers, money transmitters, lenders, mortgage brokers, and insurance companies.[158]

In response to increased cybersecurity threats to financial systems by nation-states, terrorist organizations, and criminals, the NYDFS issued its Cybersecurity Requirements for Financial Services Companies (Cybersecurity Regulation) in March 2017, which required entities regulated by the NYDFS to certify compliance with requirements for certain cybersecurity controls.[159] The first deadline for compliance was in February 2018.[160] The NYDFS Cybersecurity Regulation implements five stages of increasing requirements over a number of years to allow organizations sufficient time to make changes to their policies, procedures, and technology to comply with the minimum standards.[161]

The first stage requirements include: (1) a cybersecurity program based on risk assessments; (2) a written cybersecurity policy; (3) designation of a Chief Information Security Officer (CISO); (4) limits on user access privileges; (5) in-

156. *Id.* at 4.

157. *Id.* at 7.

158. *Who We Supervise*, N.Y. DEP'T OF FIN. SERV., https://dfs.ny.gov/who_we_supervise.

159. N.Y. Comp. Codes R. & Regs. tit. 23, § 500.00, https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf.

160. *Id.* at § 500.12.

161. Steven R. Chabinsky et al., *Sign and Submit by February 15, 2018: NYDFS Cybersecurity Certification Due Date Nears as Additional Compliance Requirements Close In*, WHITE & CASE TECH. NEWSFLASH (Jan. 24, 2018), https://www.whitecase.com/publications/article/sign-and-submit-february-15-2018-nydfs-cybersecurity-certification-due-date.

cident response plans; and (6) breech notification to the NYDFS within 72 hours.[162]

The second stage requirements add: (1) annual written report to the organization's senior leadership; (2) penetration testing and vulnerability assessments; (3) documented risk assessments; (4) use of multi-factor authentication; and (5) regular cybersecurity awareness training.[163]

Stage three includes additional granular requirements on the cybersecurity controls and monitoring, while stage four adds, among other controls, that the regulated organization implement due diligence and contractual protections with third-party service providers that form part of the supply chain.[164]

Though limited on paper to entities regulated by the NYDFS, such regulations can have the effect of improving cybersecurity nationwide.[165] According to one commentator:

> New York's Cybersecurity Rules may become a de facto national cybersecurity standard with global reach. Covered Entities have interconnected systems. Many large institutions gain efficiencies by deploying centrally managed information technology platforms and cybersecurity programs and tools. Thus, if only a part of an organization falls under the Cybersecurity Rules, it would be impractical for the larger enterprise not to adhere to the Cybersecurity Rules.[166]

Regulated utilities operate in much the same way, with service companies providing IT and other services to subsidiary regulated utilities owned by the parent company.[167]

> In the absence of leadership from the federal government on certain issues related to cybersecurity and data protection, states like New York are beginning to fill the void. Several cybersecurity experts told Business Insider that the NYDFS regulations could become a model for other industries or even policies at the national level.[168]

Widespread adoption of these types of rules will help ensure smaller organizations rise to the cybersecurity posture of larger organizations.[169]

---

162. *Id.*

163. *Id.*

164. *Id.*

165. *Id.*

166. Jon Neiditz, *Cyber Winter is Here, and Coming to Regulation: The New York Rules and the Future of Cybersecurity Regulation*, KILPATRICK TOWNSEND INSIGHTS: ALERTS (Sept. 27, 2017), http://www.kilpatricktownsend.com/en/Insights/Alert/2017/9/Cyber-Winter-is-Here.

167. LAZAR, *supra* note 73, at 32.

168. Brennan Weiss, *New York is quietly working to prevent a major cyber attack that could bring down the financial system*, BUSINESS INSIDER (Feb. 25, 2018), http://www.businessinsider.com/new-york-cybersecurity-regulations-protect-wall-street-2018-2.

169. John Herzfeld & George Lynch, *Looming N.Y. Cybersecurity Deadline Puts Pressure on Companies*, BLOOMBERG NEWS (Feb. 12, 2018), https://www.bna.com/looming-ny-cybersecurity-n57982088661/ ("Large financial institutions with mature cybersecurity programs should be in good shape for the compliance certification deadline, but smaller companies may be struggling to meet it, Rocco Grillo, a cybersecurity global leader at Stroz Friedberg LLC, a New York-based cybersecurity consulting subsidiary of Aon Plc, told Bloomberg Law.").

Some ripples were created by the NYDFS Cybersecurity Regulation. The National Association of Insurance Commissioners also adopted, in October 2017 (National Cybersecurity Awareness Month), the Insurance Data Security Model Law (Model Law).[170] The Model Law appears to be modeled on the NYDFS Cybersecurity Regulation.[171] The Model Law creates rules concerning information security and risk assessment, oversight of third-party service providers, and investigation and notification to state regulators of breaches.[172]

Such actions at the state level can also prompt federal attention on the issue. In a report issued in October 2017, the U.S. Department of Treasury released a Report that included references to the Model Law, and

> recommends prompt adoption of the NAIC Insurance Data Security Model Law by the states. Treasury further recommends that if adoption and implementation of the Insurance Data Security Model Law by the states do not result in uniform data security regulations within five years, Congress pass a law setting forth requirements for insurer data security, but leaving supervision and enforcement with state insurance regulators."[173]

Data security and breach notification laws have been enacted at the state level.

> However, data security, data breach notifications, and more broadly, cybersecurity are also issues of national concern. U.S. insurers should be subject to the same requirements for cybersecurity and protection of PII and PHI regardless of where they are domiciled and operate, and U.S. policyholders should be able to expect the same level of protection of their personal data regardless of where they live.[174]

Whatever the merits of such comprehensive regulation, once one governmental entity introduces such a scheme, others will typically follow.[175] High profile breaches continue in almost every market segment.[176] Energy critical infrastructure, specifically, have received heightened levels of publicity concerning alleged cyber intrusion attempts.[177] These events draw the attention of legislators and regulators, and prompt action to respond to the increased cybersecurity threats to critical infrastructure by nation-states, terrorist organizations, and crim-

---

170. *NAIC Passes Insurance Data Security Model Law*, NAT'L ASS'N INS. COMM'RS (Oct. 24, 2017), http://www.naic.org/Releases/2017_docs/naic_passes_data_security_model_law.htm.

171. *NAIC Model Laws, Regulations, Guidelines and Other Resources—4th Quarter 2017*, NAT'L ASS'N. INS. COMM'RS, http://www.naic.org/store/free/MDL-668.pdf (explaining "[t]he drafters of this [Model] Act intend that if a Licensee . . . is in compliance with [the NYDFS Cybersecurity Regulation], such Licensee is also in compliance with this [Model] Act.").

172. NAT'L ASS'N INS. COMM'RS, *supra* note 170.

173. Steve T. Mnuchin & Craig S. Phillips, *A Financial System That Creates Economic Opportunities: Asset Management and Insurance*, U.S. DEP'T OF TREASURY, at 117 (Oct. 2017), https://www.treasury.gov/press-center/press-releases/Documents/A-Financial-System-That-Creates-Economic-Opportunities-Asset_Management-Insurance.pdf.

174. *Id.*

175. Steve Livingston et al., *Managing cyber risk in the electric power sector*, DELOITTE (Jan. 31, 2019), https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/cyber-risk-electric-power-sector. html.

176. Kevin Townsend, *Cyberattacks Against Energy Sector Are Higher Than Average: Report*, SECURITYWEEK (Nov. 1, 2018), https://www.securityweek.com/cyberattacks-against-energy-sector-are-higher-average-report.

177. *Id.*

inals.[178] As the insurance industry and utilities industry share certain attributes—such as being highly interconnected and heavily regulated—the design, implementation, and subsequent response to the NYDFS cybersecurity regulations could be informative to the utilities industry.[179]

3. Existing Approaches: Industry Standards

In addition to governmental efforts, "cybersecurity issues are largely governed by a series of standards that do not have the force of law but are widely used and instructive."[180] The National Institute of Standards and Technology (NIST) publishes the Cybersecurity Framework (CSF).[181] The International Organization for Standardization (ISO) publishes the ISO 27000 series on information security management systems.[182] The alphabet soup continues ad nauseam.

While the landscape has changed somewhat after several high profile breaches, vendors appear to still be focused more on getting products to market rather than taking the time to design products with security considerations that are embedded into the design of the product itself.[183] As the electric sector deploys smart grid technology that involve "third-parties to design, develop, and install the devices, it will be increasingly important for boards and management to be assured that such 'progress' is not progressively making the company's operations more susceptible to advanced persistent attacks by creating vulnerabilities adversaries could exploit."[184]

"Despite these vulnerabilities, many power companies are doubling down on the danger; they are implementing 'smart grid' technologies that give their IT systems more control over the delivery of power to individual customers—or even to individual appliances in customers' homes. . . . But security is not a priority for smart grid designers," many of whom see it as a last box to check before rapidly introducing the product to market.[185]

III. ARGUMENT

Legislatures and regulators will undoubtedly react to a successful cyberattack on the US electric grid by introducing additional regulations. Rather than be distracted by disagreement over the relative merits of risk-based and compli-

178. Livingston, *supra* note 175.

179. Mnuchin, *supra* note 173, at 117.

180. Anderson, *supra* note 123.

181. *Cybersecurity Framework*, U.S. DEP'T OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., https://www.nist.gov/cyberframework.

182. *Information technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary*, INT'L. ORG. FOR STANDARDIZATION, INT'L STANDARD (5th ed. 2018), https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip.

183. Stewart Baker et al., *In the Dark: Crucial Industries Confront Cyberattacks*, CTR. FOR STRATEGIC & INT'L STUDIES (Apr. 19, 2011), https://perma.cc/2V5V-8JDP.

184. Trope, *supra* note 38, at 776.

185. Baker, *supra* note 183.

ance-based approaches to addressing cybersecurity, an opportunity exists to deconflict the approaches and for the industry to proactively engage governmental entities in creating minimum cybersecurity requirements that are flexible, sensible, and acceptable to all stakeholders. Neither approach is sufficient on its own. Compliance sets a minimum standard that is important but remains static and is not ideal for a shifting landscape. Risk-based approaches are much more dynamic in nature and allow for timely responses to evolving threats, but do not inherently establish minimum requirements as they are subject to interpretation. Risk-based approaches are also not ideal for entities that do not have the cybersecurity maturity or sophistication to implement a comprehensive risk-based approach. Rather than the false dichotomy between risk-based and compliance-based approaches, we suggest they can coexist, with minimum cybersecurity requirements setting a "floor" upon which risk-based approaches allow the sophisticated entities to build upon and excel.

A. History of Legislative and Regulatory Reponses to Perceived Threats

According to a 2017 Accenture report, the majority of utility executives believe cyberattacks could cause disruptions to distribution grids in the near future.[186] "History shows that when the United States is attacked, our government responds with legislation that is designed to secure our assets, protect our people, and prevent such attacks from occurring again."[187] Such a reaction is also likely in response to any large-scale blackouts caused by cyber disruption.[188] "Thus far, cybersecurity breaches in the United States have not resulted in death or severe damage to our national security or critical infrastructure, but the threat is substantial and common consensus is that a successful attack with severe results is on the horizon."[189] Some commentators have said that such a debate about whether additional regulation is necessary is moot, as they are inevitable in response to cyber caused disruptions.[190]

These conversations are far from hypothetical for the utilities sector. In response to the 2013 physical attack on PG&E's Metcalf Transmission Substation, the California PUC issued an order in January 2019 extending NERC CIP-014-like physical security requirements on distribution utility systems.[191]

---

186. Eduard Kovacs, *Utilities Fear Cyberattacks Could Cause Electric Grid Disruptions: Survey*, SECURITYWEEK (Oct. 5, 2017), https://www.securityweek.com/utilities-fear-cyberattacks-could-cause-electric-grid-disruptions-survey.

187. Laughlin, *supra* note 104, at 346 (2016).

188. *Id.* at 346-47, 362, 370.

189. *Id.* at 346–47.

190. *Id* at 351. "As such, the debate about whether there must be additional laws or regulations requiring companies to take certain actions continues. That debate is moot. The current patchwork of cybersecurity laws and regulations is not sufficient to protect U.S. national security. Additional cybersecurity laws and regulations are not just necessary, they are inevitable. Thus, private companies, Congress, and agencies should focus on developing them in a way that ensures a high level of protection and promulgating them before a major attack occurs." *Id.*

191. *Order Instituting Rulemaking Regarding Policies, Procedures & Rules for Regulation of Physical Sec. for the Elec. Supply Facilities of Elec. Corps. Consistent with Pub. Utilities Code Section 364 & to Estab-*

B. False Dichotomy of Risk v. Compliance

While often presented as opposing and incompatible approaches, risk and compliance frameworks do not have to exist as mutually exclusive options. Instead of viewing risk-based and compliance-based approaches as alternatives, we should look for more synergies and opportunities to use them in a complementary manner.

The NIST CSF, the result of collaboration between government and the private sector, is widely considered as a prime example of a risk-based framework.[192] However, within this risk-based framework, the NIST CSF contemplates the organization's regulatory and legal requirements as components of risks to be addressed.[193] It specifies that those requirements form the understanding to "inform the management of cybersecurity risk."[194] Specifically, ID.GV-3 within the NIST CSF Framework states that "[l]egal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed." [195] The framework recommends an organization put a process in place to address both legal and regulatory requirements.[196] That is, legal and regulatory requirements are treated as a risk to be addressed. The NIST CSF integrates risk-based and compliance-based approaches to achieve better overall security while addressing both structure and flexibility.[197]

Similarly, the NERC CIP is often presented as an example of a compliance-based approach[198]—specific metrics accompanied by large fines for noncompliance.[199] However, at the core NERC CIP reliability standards is a categorization of cyber assets and systems based on risk factors, which determines the requirements that those assets are then subject to.[200] NERC CIP does not uniformly apply all requirements to all assets.[201] Instead, assets are categorized by the potential impact their disruption can have on the system.[202] As such, the most stringent requirements only apply to "facilities, systems, and equipment which, if

---

lish Standards for Disaster & Emergency Preparedness Plans for Elec. Corps. & Regulated Water Companies Pursuant to Pub. Utilities Code Section 768.6., D. 19-01-018, 2019 WL 398286, (Cal. P.U.C. Jan. 10, 2019) http://docs.cpuc.ca.gov/PublishedDocs/Published/G000/M260/K335/260335905.PDF.

192. Rick Tracy, *A Tale of Two Frameworks: The NIST CSF and NIST RMF Are Not the Same*, TELOS CORP. (May 18, 2017), https://multimedia.telos.com/blog/tale-of-two-frameworks-nist-csf-and-nist-rmf-confusion.

193. *Framework for Improving Critical Infrastructure Cybersecurity*, NAT'L INST. OF STANDARDS & TECH. 26 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

194. *Id.* at 25.

195. *Id.* at 26.

196. *Id.* at 4.

197. *Id.* at 11.

198. *2018 Staff Report: Lessons Learned from Commission-Led CIP Reliability Audits*, FED. ENERGY REG. COMM'N 4 (Mar. 29, 2019).

199. N. AM. ELEC. RELIABILITY CORP., *supra* note 74; Smith, *supra* note 74.

200. *Cyber Security—BES Cyber System Categorization*, N. AM. ELEC. RELIABILITY CORP. https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf (last visited Sept. 7, 2019).

201. *Id.*

202. *Id.*

destroyed, degraded, misused, or otherwise rendered unavailable,"[203] would have the most effect on the reliable operations of the grid.

C. A Risk-Based Approach Is Not Sufficient on Its Own

Proponents of risk-based approaches should acknowledge the value of applying an underlying compliance-based structure, which promotes compliance with minimal requirements, permits targets to be met, and auditors to report on progress. However, businesses ultimately must make a choice on how much risk to accept and where to allocate their resources. There is a risk that, without some minimum compliance requirement, some companies will choose to assume the risk in certain scenarios.

> Under a risk-based cybersecurity approach, private companies determine the probability of cyberattacks occurring at various levels of magnitude and the costs and measures necessary to prevent each type of attack. When the costs to protect the company from an attack outweigh the costs to recover from an attack, companies are typically willing to accept the risks rather than invest in protecting against them.[204]

Many smaller companies, especially small and medium size utilities, may perceive the risk of a cyber attack as too small as they do not consider themselves an attractive target, due to the presumed lack of interest in their operations or the impact they may have on the larger system. However, those entities may underappreciate the value of their systems as the testing environment in which threat actors can learn about utility operations, as well as develop and refine their techniques. The supply chain upon which utilities rely also include small companies which present similar risks. These smaller entities may also believe, erroneously, that they are too small to be targeted, or the cost to protect themselves may exceed the perceived benefit. Regardless of the reason, these companies can serve as the soft underbelly through which to gain access to and disrupt operations to larger organizations.

"[I]nstitutions should first comply with essential practices, known to be effective and efficient, and use 'risk management' for making exceptional decisions and justifying expensive measures."[205] Smaller, less well-resourced institutions are being asked to "use risk assessments that most do not have the necessary knowledge, skill, abilities, and experience to make. In the meantime, the environment has become far more hostile than might have been expected."[206]

The types of cyber threats faced by utilities, especially those coming from Advanced Persistent Threats (APTs),[207] are high impact but low probability.

---

203. *Id.*

204. Laughlin, *supra* note 104, at 357-58.

205. *Improving Cybersecurity in the Healthcare Sector*, 21 SANS NEWSBITES (Apr. 3, 2019), https://www.sans.org/newsletters/newsbites/xxi/28.

206. *Id.*

207. An Advanced Persistent Threat (APT) is "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors. . . . [and] establishing and extending footholds within the information technology infrastructure

APTs do not engage in the conventional cost-benefit analysis generally undertaken by businesses, as their focus could be on economic, geopolitical, ideological, strategic, or other non-monetary considerations.[208]

Threats identified using a risk-based approach will be triaged, and not all threats will receive the same level of required attention and remediation.[209] However, the triage means the approach is unlikely to perfectly align with all potential threats, particularly high impact low probability events.[210] This is one reason why a compliance-based approach is needed to assure there are measurable minimum-levels of security in place.[211]

> Private companies also lack incentive to invest in protecting against APTs because they do not internalize the negative and positive externalities of a successful cyberattack. For example, if a cyberattacker disables a power generation facility, the operator may have to invest in new computer systems and infrastructure and it will lose some revenue from its customers. However, the federal government will step in to assist with getting the systems operational and finding the perpetrator. The people who would suffer the most are those without power.[212]

These potentially unaccounted for externalities are squarely within the expertise of policy makers to consider.

D. A Compliance-Based Approach Is not Sufficient on Its Own

Often compliance-based security is derided as leading to "check box" security, in which entities will believe they are secure simply because they have checked the boxes by implementing (only) the required controls under a compliance regime.[213] Compliance-based approaches alone do not permit an entity the flexibility to "think like a black hat" and address, in a targeted and efficient manner, the most pressing concerns that are most likely to be leveraged by threat actors.[214]

This topic is well covered, and the broader cyber community has shifted persistently from compliance-based to risk-based security over the past dec-

---

of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives." *Advanced Persistent Threat (APT)*, NAT'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/advanced-persistent-threat (last visited Sept. 7, 2019). APTs are often associated with nation-states that seek to disrupt military or intelligence operations, or businesses seeking a competitive advantage. *What Is an Advanced Persistent Threat (APT*)?, CISCO (last visited Sept. 7, 2019), https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html.

208. CISCO, *supra* note 207.

209. *Id.*

210. *Id.*

211. *Id.*

212. Laughlin, *supra* note 104, at 357-58.

213. *Compliance-based security risky, says SecureWorks*, COMPUTER WEEKLY (Mar. 17, 2010), https://www.computerweekly.com/news/1280092383/Compliance-based-security-risky-says-SecureWorks.

214. *Id.*

ade.[215] Much of the industry views compliance requirements as unnecessary burdens legislated into existence by entities who do not fully understand the day to day operations of security professionals.[216] It is true that compliance-based approaches alone are not enough.[217] However, compliance-based approaches are a necessary piece of the security puzzle.[218]

E. Floor, not Ceiling

Compliance-based approaches should be considered the "floor" of security throughout the industry, ensuring all entities adhere to a minimum set of practices to protect consumers. In the energy sector, consumers often do not have a real choice as to the service provider and must have some minimum level of security they can rely on.[219] Furthermore, entities with sophisticated and mature cybersecurity programs are interconnected both electrically and through the supply chain of vendors to each other, with overall security implicitly dictated by the weakest link in the chain.[220] Risk-based approaches can then build on and enhance the security posture of the utility together with that floor set by the compliance-based approaches. Incorporating risk mitigation considerations into that approach, entities can experiment and excel, developing specific and efficient interventions for specific environments, sectors, entities, departments, functions, locations, and whatever other level or combination of granularity.[221]

Some entities mistakenly treat compliance-based security as the ceiling, rather than the floor, which could lead to serious security vulnerabilities.[222] Between 2016 and 2018, FERC staff conducted audits to evaluate compliance with NERC CIP Reliability Standards.[223]

> During the audits, staff found that most of the cyber security protection processes and procedures adopted by the registered entities met the mandatory requirements of the CIP Reliability Standards. However, there were also potential compliance infractions found. Additionally, staff noted observations of practices that could improve security but are not necessarily required by the CIP Reliability Standards.[224]

---

215. Joel Griffin, *Shifting from compliance-based IT security to a risk-based model*, SEC. INFOWATCH (Mar. 18, 2013), https://www.securityinfowatch.com/cybersecurity/information-security/article/10895722/wisegate-publishes-report-on-the-importance-of-having-a-riskbased-it-security-program.

216. Frank Ohlhorst, *Risk, Compliance and security management go hand in hand*, TECHREPUBLIC (June 11, 2014), https://www.techrepublic.com/article/risk-compliance-and-security-management-go-hand-in-hand.

217. Griffin, *supra* note 215.

218. Ohlhorst, *supra* note 216.

219. *Id.*

220. *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*, NAT'L RESEARCH COUNCIL (Nat'l Academy Press 2002), https://citadel-information.com/wp-content/uploads/2012/08/cybersecurity-today-and-tomorrow-pay-now-or-pay-later-national-research-council-2002.pdf.

221. Ohlhorst, *supra* note 216.

222. *Id.*

223. FED. ENERGY REG. COMM'N, *supra* note 198, at 4.

224. *Id.*

Not only were compliance infractions found, but there are many practices that would improve security but are not required by CIP.[225] In fact, some of the biggest, well-resourced utilities that presumably have the resources to "do it right" have been caught with lackluster security in certain isolated situations. In January 2019, Duke Energy was fined $10 million dollars for 127 violations of NERC CIP Reliability Standards.[226] Duke is one of the largest electric power holding companies in the United States and provides electricity to 7.6 million retail customers in six states, with "approximately 51,000 megawatts of electric generating capacity."[227] The filing notes the violations "posed a serious risk to the security and reliability" including "repeated failures to implement physical and cyber security protections" and allowing vendors without proper clearance to gain unescorted access to sensitive locations such as substations and server rooms.[228]

Anonymized reports and sharing can "inform[] the regulated community and the public of additional lessons learned . . . provide[] information and recommendations" that are useful in assessments of risk, compliance, and to overall cyber security, as well as be generally beneficial to the utility-based cyber security community to improve security.[229]

Perhaps regulators should combine their creation of minimum expectations for utility behavior with incentives for going beyond those requirements and combining traditional compliance-based frameworks with more creative advanced risk-based compliments to those necessary foundational expectations. Creating incentives based on achievement of exceptionally secure environments, peer review arrangements, and third-party expert feedback could be a solid complement to setting minimum standards and only measuring achievement of those requirements.

In fulfilling their role of ensuring the cybersecurity posture of utilities, regulatory entities deal with the same challenges of identifying, hiring, training, and retaining staff with the necessary skillset.[230] PUCs may alternatively rely on third-party auditors to assist with conducting comprehensive compliance audits and assessments.[231] In either case, interpreting the utilities' cybersecurity posture is a significant and complex undertaking.

A recent FERC Staff audit report indicated the complexity surrounding the oversight process.[232] A FERC staff audit of registered entities involved

> data requests to gather information pertaining to an entity's CIP activities and operations . . . webinars and teleconferences to discuss the audit scope and objectives,

225. *Id.*

226. N. AM. ELEC. RELIABILITY CORP., *supra* note 74; Smith, *supra* note 74.

227. *What We Do*, DUKE ENERGY, https://www.duke-energy.com/our-company/about-us (last visited Sept. 7, 2019).

228. FED. ENERGY REG. COMM'N, *supra* note 198, at 4.

229. *Id.* at 5.

230. *Id.* at 4.

231. *Id.*

232. *Id.* at 7.

> data requests and responses, technical and administrative matters, and compliance concerns. During a site visit, staff interviewed an entity's subject matter experts; observed operating practices, processes, and procedures used by its staff in real-time; and examined its functions, operations, practices, and regulatory and corporate compliance culture.[233]

In addition, "staff interviewed employees and managers responsible for performing tasks within the audit scope and analyzed documentation to verify compliance with requirements; conducted several field inspections and observed the functioning of applicable Cyber Asset[s] . . . and interviewed compliance program managers, staff, and employees responsible for day-to day compliance and regulatory oversight."[234] It is by no means a simple undertaking.

Even with the compliance-based approaches sometimes criticized as overly prescriptive, not all entities will meet basic requirements. For example, in the 2018 Staff Report, FERC identified several basic practices that were not consistently used at registered entities.[235] It included: (1) use of expired security certificates when accessing webservers internally;[236] (2) use of less secure encryption strength;[237] (3) use of components that have reached "end-of-life" and were no longer supported by vendors;[238] (4) inconsistent use of file verification to protect against supply chain attacks delivered through malicious software or firmware updates;[239] (5) inaccurate asset inventory baselines;[240] and (6) lack of identification of sensitive information and "documented method for responding to data loss events."[241]

If minimum standards are not being uniformly followed across the industry, then imagine what would happen if we moved to a completely risk-based envi-

---

233. FED. ENERGY REG. COMM'N, *supra* note 198, at 7.

234. *Id.*

235. *Id.* at 9.

236. *Id.* at 11-12. While this by itself presents minimal security vulnerability from technical exploitations, it allows users to become accustomed to connections that present a security certificate error, which may desensitize the users and make them more susceptible to social engineering attacks. *Id.* at 11-12.

237. FED. ENERGY REG. COMM'N, *supra* note 198, at 13. Where stronger encryption would have involved a simple configuration change without the need for new hardware or software. *Id.*

238. *Id.* at 15-16. There is some disagreement over this practice, as many systems are considered air gapped, and many security professionals consider air gapped legacy systems to be at minimal risk, but there is little reason not to require something along the lines of "in all practical scenarios replace end of life components." *Id.*

239. *Id.* at 16. The risk was vividly illustrated by ASUS update utility exploitation in 2019 and the Cleaner supply chain exploitation. *Id.*

240. FED. ENERGY REG. COMM'N, *supra* note 198, at 17. Which is of particular concern as it is impossible to protect assets if it is not known to the organization what assets it holds, as vividly illustrated by the Sony and OPM breaches. Again, it is difficult to imagine sound objections to a requirement that entities should maintain an up to date inventory of assets, without dictating implementation of any specific technology or method for maintaining such an inventory. *Id.*

241. *Id.* at 20. Similarly, it is difficult to protect information if there is no identification of what information is sensitive. However, it must be recognized that labeling of sensitive information is a particularly intractable problem, especially with the exponential increases in information produced. On the other hand, having a documented method for responding to data loss events is a must. *Id.*

ronment. What would security look like across the utility industry? Some entities would still invest heavily in appropriate security measures, but we fear more entities might choose to accept additional levels of risk. So, what would the situation be like if no compliance-based regime existed to establish this basic level of security? Is it plausible or logical to suggest the same entities who did not meet these basic practices under a compliance-based regime would institute these basic practices if less was required of them? Logic would suggest not. These gaps in cybersecurity implementations may be the result of the mistake of treating compliance-based requirements as setting the "ceiling" rather than the "floor" for cybersecurity.

A sensible set of minimum cybersecurity requirements on critical infrastructure should not be seen as an opening for government to direct all cybersecurity efforts of critical infrastructure operators and second guess day-to-day business decisions. The public has a reasonable expectation that decisions are made with their best interest in mind. As a result, regulators will continue to establish achievable but necessary compliance-based requirements to set the floor upon which the industry must stand to avoid current security risks.[242] Even though

> [t]he private sector places high value on a non-statutory and non-regulatory risk-based approach[,] [c]ompanies generally share a concern that a government solution would increase expenses, misallocate resources, focus on compliance, decrease public-private partnerships, and ultimately result in little to no actual cybersecurity benefits. . . . While technological developments move quickly, it can take years for the government to create new laws and regulations. [243]

The result is an ongoing tension between regulators and utilities that are trying to find the right balance that both promotes and supports appropriate behavior but also avoid unnecessary allocation of resources toward activities that do not really improve overall security.[244]

Government should not mandate practices that will become obsolete before they are enacted. However, there should be some requirements identified or processes designed that can be somewhat flexible, representing things that the companies doing cybersecurity well are already doing. Irrespective of the risk-based only advocates, utilities that are trailing behind should be required to implement those requirements or processes.[245]

Properly applied risk-based approaches promote excellence, serving as a framework under which utilities can continuously evolve and adapt. Risk-based approaches, however, are simply not enough on their own.[246] As one commentator acknowledged: "These voluntary measures could be made even stronger by the introduction and passage of formal legislation streamlining the information

242. Laughlin, *supra* note 104, at 351.

243. *Id.* at 358-59.

244. *Id.*

245. *Id.* at 361-62.

246. Hellmann, *supra* note 130, at 178.

sharing process and providing liability and privacy protection . . . which would further incentivize industry participation."[247]

> Rather than wait for an attack to occur to spark implementation of cyber security measures in SCADA systems, the government -- working alongside private industry -- should be proactive, anticipating the storm to come. [Energy] resources should be more protected from destruction through the best voluntary cybersecurity programs possible, thereby guarding the American people from the consequences that might result from a large-scale pipeline cyber attack. To pretend that a devastating attack is not forthcoming because one has not yet succeeded is to regress to a mindset that was only practical before the advent of terrorist groups, the rise of modern technology, and the popularity of anonymous cyber activity.[248]

Currently, there is an opportunity to deconflict risk-based and compliance-based approaches. Instead, all stakeholders should promote a culture of collaboration and coordination. While many entities have the motivation to do things right, and avoid reputational, financial, and productivity damages, for others the calculus may not line up as perfectly with the interests of captive consumers.

IV. POTENTIAL OPPOSITION

This article advocates for a complementary role between compliance-based and risk-based approaches (with the former setting the floor for the latter to build upon and exceed through flexibility and creativity). There will, of course, be some opposition to what some might label an oversimplification of the impact of compliance requirements and a minimization of and mischaracterization of the likely risk acceptance determinations articulated. This section anticipates and provides responses to some of those objections, including: whether compliance-based and risk-based approaches will lead to conflicting recommendations and practices; whether compliance-based approaches offer the flexibility to address everchanging threats; the theory that inaction is better than misdirected action; and finally, whether focus should be on response rather than prevention.

A. Will Compliance-Based and Risk-Based Approaches Inevitably Lead to Conflicting Recommendations and Practices?

Some will argue that compliance-based and risk-based approaches are incompatible because a combination of both will inevitably lead to conflicting recommendations and practices.[249] This ignores the clear opportunity and efficiencies that arise by allowing both approaches to work in concert. Conflicts arise when stakeholders take a zero-sum approach to making security decisions.[250] Arguably, well-articulated risk-based approaches can comply with minimum standards. But in some cases, risk-based approaches do not comprehensively achieve minimum standards. In those circumstances, a compliance-based approach is needed as a supplement.

---

247. *Id.*

248. *Id.*

249. Ernie Hayden, *Better Safe than Compliant,* 149 No. 8 Pub. Util. Fortnightly 50, 51 (2011).

250. Hellmann, *supra* note 130, at 178.

As Ernie Hayden put in in his 2011 article on this topic:

> The combined effects of well-intentioned early action and incomplete or contradicting guidelines from various jurisdictions increases the likelihood that the policy and operational focus will remain on compliance—reporting and documentation that can be mandated and measured—rather than a more holistic, risk-based philosophy that has been used successfully in the non-utility world, and is a foundation of U.S. federal agency information security programs.[251]

There remains an opportunity to establish a baseline and make it abundantly clear that such a baseline establishes the floor, not the ceiling or the average, of utility cybersecurity achievements and accomplishments. There must be some basic level of security and certain well-established practices that are universally applicable to all utilities, regardless of size, geography, or resources. In the rare event that a system's idiosyncrasies indicate it may lessen security to implement certain practices, that utility can seek a waiver which will no doubt be granted.[252] But history suggest those situations are rare.[253]

Though it is difficult, stakeholders should collaboratively craft compliance-based approaches sensibly, so as not to dictate specific products or configurations. Moreover, interpretations and enforcement of compliance-based approaches should not be inflexible and should incorporate intentions of the drafter so as not to lead to illogical or absurd implementations. That is why NERC enforces its standards in a risk aware manner.[254] Not all incidents of noncompliance lead to penalties.[255]

When NERC Reliability Standards were first introduced, they were enforced uniformly, regardless of the level of risk that instances of noncompliance actually present to the reliable operations of the grid.[256] However, NERC has steadily shifted towards risk-informed enforcement of the reliability standards. In 2012, NERC introduced "Find, Fix & Track," under which incidents of noncompliance that pose less risk must still be remediated and documented, but will not involve a monetary penalty or the traditional Notice of Penalty.[257] In 2015, FERC approved NERC's risk-based Compliance Monitoring and Enforcement Program (CMEP) to allow entities to "focus time and effort on higher-risk issues while still identifying, correcting, and tracking lesser-risk issues."[258] The best

---

251. Hayden, *supra* note 249, at 51.

252. *Id.*

253. *Id.* at 52.

254. *Id.* at 51.

255. *Id.* at 52.

256. Burt, *supra* note 107.

257. Stephen M. Spina & J. Daniel Skees, *FERC Grants NERC Enforcement Discretion over Low-Risk Violations*, MORGAN LEWIS LAW FLASH (Mar. 16, 2016), https://www.morganlewis.com/pubs/energy_lf_fercapprovesenforcementlow-riskviolations_16mar12.

258. *North American Electric Reliability Corporation*, 150 F.E.R.C. ¶ 61,108 at P 7 (2015); "It is not practical, effective, or sustainable to monitor all compliance issues to the same degree or treat all noncompliance in the same manner. A risk-based approach to compliance monitoring is based on a number of considerations, including risk factors, and registered entity management practices related to the detection, assessment, mitigation and reporting of noncompliance. A risk-based approach enables proper allocation of resources from

regulatory frameworks can direct expected behavior in a way that allows the regulated entity to outperform those expectations and not be constrained by them.

Ultimately, it is better to have some sort of coordination than to end up with multiple standards across the states, especially for companies with shared services that span multiple jurisdictions. "Lack of coordination among multiple federal, state and regional jurisdictions asserting authority over smart grid security is also likely to generate confusion, conflicts and unsupported confidence in system security."[259]

B. Are Compliance-Based Approaches Flexible Enough to Protect Against Ever-Changing Threats?

Some argue that compliance-based approaches are not flexible enough to protect against the ever-changing security threats.[260]

> Unfortunately, a compliance checklist approach . . . might inherently lack the scope and adaptability needed to counter digital adversaries' continually emerging and evolving strategies and tactics. In other words there's a tendency by regulators and legislators to enforce security through compliance with . . . standards and not necessarily to focus on protecting the most critical assets or addressing the highest cyber risks.[261]

"Hackers don't have checklists" and "utilities can't think they're secure by simply checking off a list of compliance requirements."[262] However, birds don't have checklists either, but when operating an airplane pilots use checklists to ensure the plane is optimally prepared to prevent and, if required, survive a bird strike. It does not mean every pilot who follows a checklist will prevent or recover from potential bird strikes flawlessly, but it does ensure some minimum level of competency among the pilots permitting them to avoid or minimize unwanted contact between plane and bird. Minimum requirements are especially appropriate where the population of vulnerable entities are not equally adept.[263] Moreover, such minimum requirements can easily fit into a larger scheme that allows for innovation that exceed those requirements.

"Industry members have vocalized that changing this relationship between government and industry to one of 'regulator-regulated' would force companies to focus more resources on compliance rather than development of robust cybersecurity programs, hindering implementation of new measures."[264] While certain

---

both the Regional Entity and registered entity for compliance monitoring, and encourages registered entities to enhance internal controls, including those focused on the self-identification of noncompliance." NPCC Entity Risk Assessment Program Guide for Risk-based Compliance Monitoring and Enforcement Program, NE. POWER COORDINATING COUNCIL 2 (Mar. 2, 2015), https://www.npcc.org/Compliance/Entity%20Risk%20Assessment/NPCC_ERA_Program_Guide_Rev1_032615.pdf.

259. Hayden, *supra* note 249, at 51.

260. Hellmann, *supra* note 130, at 174.

261. Hayden, *supra* note 249, at 51.

262. *Id.* at 50.

263. Hellmann, *supra* note 130, at 175.

264. *Id.*

entities with sophisticated and mature cybersecurity programs likely feel that they do not need regulatory oversight,[265] those same entities should agree that certain minimum levels of security must be maintained by everyone in the industry, and the mostly likely way for that to occur is some form of compliance-based regulation.

As Hillary Hellmann points out in a 2011 review:

> There are, nevertheless, some benefits to formal regulation. The mandatory regulations issued by the North American Electric Reliability Corporation (NERC) under the guidance of the Federal Energy Regulatory Commission (FERC) to regulate the cyber security of the electric grid, for example, have forced private entities to increase their cybersecurity standards, ensuring the grid's durability. Compliance is verified, and the FERC is able to conduct the appropriate oversight, review, and approval of all activities. Penalties for non-compliance can be harsh but effective.[266]

Entities subject to NERC Reliability Requirements already cope with some mandatory requirements on parts of their systems and have implemented practices beyond those required.[267]

Other industry stakeholders have instead advocated for regulators to "adopt a performance-based oversight and assessment scheme to focus on a utility's actual security posture and performance, rather than on the quality or content of its supporting paperwork. In other words, utilities should first spend their resources on identifying and protecting the critical assets, then complete the . . . paperwork."[268]

Performance in cybersecurity is difficult to assess without standards. While some metrics have been developed and are being refined, performance-based oversight brings its own set of challenges.[269] Performance assessments cannot be based on breaches, as breaches do not necessarily suggest irresponsible behavior prior to the breach.[270] Often breaches happen despite responsible behavior prior to the breach.[271] Yet metrics focused on implementation level of controls quickly begin to resemble compliance-based regimes.[272]

As noted earlier, hackers do not have checklists, and only need to find a small flaw to gain a foothold in a system.[273] In contrast, defenders need to protect the entire system.[274] Hindsight review based on performance would be un-

265. *Id.*

266. *Id.*

267. *United States Mandatory Standards Subject to Enforcement*, N. AM. ELEC. RELIABILITY CORP., https://www.nerc.com/pa/Stand/Pages/ReliabilityStandardsUnitedStates.aspx (last visited Sept. 3, 2019).

268. Hayden, *supra* note 249, at 52.

269. *Id.* at 50-51.

270. Nancy Brockway, *Security and the States*, 150 No. 7 PUB. UTIL. FORT. 34 (2015).

271. Hayden, *supra* note 249, at 52.

272. *Id.* at 50.

273. *Id.*

274. *Id.* at 51.

fair to high value targets potentially dealing with well-resourced advanced persistent threats with nation-state backing.[275]

> Delays and uncertainties that are commonplace in regulatory rulemaking processes carry extraordinary costs to entities in the context of cyber security. CIP Standard requirements impose tremendous administrative and logistical burdens on regulated entities. Large utilities must implement logical and physical mechanisms to secure thousands of devices spread across hundreds or thousands of miles of infrastructure. Delays and uncertainties carry significant costs in terms of planning and deployment required to implement cyber security protections.[276]

Regulatory interventions that focus on and respond directly to the most recent cyber event (typically those resulting in a service disruption) generally fail to address the real underlying problem. Infrastructure operators, legislators, and regulators will respond to such impactful disruptions by promulgating additional compliance requirements focused on addressing a specific problem that, as a result of the incident, has likely already been addressed. Historically, those requirements directed at preventing an outcome specific to the threat or vulnerability involved in the recent incident, may result in inefficiencies if broadly implemented. To restate, such reactionary regulations may add some value but are likely to focus on a symptom rather than an underlying cause. Frequently these reactionary interventions also create uncertainty and opens a door for potentially even less desirable regulatory schemes in the future. These reactionary rules do not provide an optimal set of minimum requirements. Ideally, an evolving set of minimum requirements would be those that most mature cybersecurity programs have implemented already, or are planning to implement, and if broadly applied would only have the practical effect of improving the security posture of those in the lowest levels of cybersecurity maturity. As noted earlier, small and medium sized utilities and their vendors and then vendors to their vendors that often do not have the funding and economies of scale to implement advanced cybersecurity programs may represent a "soft underbelly" for attackers to penetrate and impact the interconnected energy systems.[277]

Stakeholders must consider any tradeoffs between enforceability, avoiding ambiguity, and enough flexibility in a sensible set of minimum requirements to accommodate anticipated cyber threats.[278]

C. If You Can't Do It Right Is It Better to Do Nothing?

Some have argued regulators do not have the expertise to provide an oversight function correctly. They suggest it is better for regulators to do nothing and leave the industry experts to ensure cybersecurity. This is both naïve and dangerous. Regulators have access to the same experts, materials, and frameworks

---

275. Yiftach Keshet, *Protecting Against Advanced Persistent Threats in 2019 and Beyond*, CYNET, https://www.cynet.com/blog/protecting-against-advanced-persistent-threats-in-2019-and-beyond/ (last visited Sept. 3, 2019).

276. Brereton, *supra* note 88, at 41.

277. Laughlin, *supra* note 104, at 361–362.

278. Brereton, *supra* note 88.

as the industry. Most of the utilities are adopting frameworks and maturity models available to everyone. It would be a mistake for regulators to get on the playing field and direct the use of specific security protocols. As some commentators have noted: "It might not be productive for a regulator, federal or state, to set design standards as the primary means to protect the smart grid."[279] "As new technologies are introduced, design requirements need to be updated" and "regulation by specific standards might give the public a false sense that the risks to the grid have been contained."[280] However, structuring compliance requirements to assure that consumers receive at least a minimal level of protection is squarely in their wheelhouse.

Perpetuating the notion that industry and regulators have different and adversarial goals is simply not productive. As Andy Bochman explains:

> There's often an assumption that utilities and regulators have conflicting interests. However, this assumption is erroneous. Both utilities and regulators have the same goals under the utility compact: to deliver safe and reliable service at a reasonable price. The difference lies in the way each side reaches the goals, or its reasons for achieving them.[281]

But collaboration between industry and regulators is essential. At a certain point, doing the best you can is better than ignoring the problem. Waiting for a perfect solution while our collective heads are in the sand is not a solution either. It is likely that inaction will lead to less coordinated actions in different states, especially in the wake of a high-profile event as legislatures and regulators react.[282]

D. Should Regulatory Policy Focus on Response, Rather than Prevention?

One open question remains: "In the absence of a uniform federal or state standard for critical infrastructure cybersecurity, by what standard will our response to this cyber threat ultimately be judged?"[283] In general, the cybersecurity experts have moved towards judging an entity by its response, rather than by whether it has suffered a cyber attack. This is because a well-resourced and motivated attacker has the potential to penetrate and disrupt even the most protected digital system. This is in great part due to the role human behavior plays in any operational context.[284] As long as human beings are involved, threat actors will be able to leverage weaknesses to their advantage.[285] The fact is, there is no perfectly secure functional system.

---

279. Brockway, *supra* note 270, at 38.

280. *Id.*

281. Bochman, *supra* note 135, at 27.

282. *See, e.g.* GDPR, CCPA, and progenies among the states.

283. Trope, *supra* note 38, at 768.

284. Fran Howarth, *The Role of Human Error in Successful Security Attacks*, SecurityIntelligence (Sept. 2, 2014) https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/.

285. *Id.*

While focus has shifted to response, rather than prevention,[286] it does not mean preventative measures are not worthwhile. Nor does it mean organizations should not be required to achieve a certain baseline level of security. Nor does it mean organizations cannot be required to have plans in place to respond to such high impact, low frequency events. It is always better to plan for and test these things under blue sky, rather than black sky, conditions. That is, a compliance-based approach can also accommodate a requirement that entities have plans in place to respond.

Regulators and legislators continue to develop a fuller understanding of emerging cybersecurity considerations and how they might impact utility operations.[287] Still there are signs of a trend towards proposing new security requirements for all critical infrastructures.[288] For example, as noted earlier, the NYDFS somewhat controversial Cyber Rules were promulgated at the end of 2016 and recently took full effect.[289] While the Federal Trade Commission (FTC) has historically taken a risk-based framework approach that is technology-neutral and relied on financial institutions to maintain their own programs,[290] the proposed updates to the Gramm-Leach-Bliley Act (GLBA) data security standards have many of the specific requirements that would be imposed by the NYDFS Cyber Rules that some commentators have called unworkable and inflexible.[291] Two FTC Commissioners have called the proposed rules overly prescriptive, premature, inflexible, and a risk of the FTC substituting its own judgment for private industry governance decisions.[292]

The industry has an opportunity to proactively advocate for collaboration among all stakeholders to deconflict compliance-based and risk-based approaches and avoid or mitigate unilateral regulatory and legislative activity that inevitably results after disruptive cyber events.[293]

V. IMPACT

The energy sector is at a critical juncture. Currently, there is an opportunity to create minimum security requirements across industries that are sensible and impose minimal expectations on entities already doing cybersecurity well, while raising the maturity levels of additional entities that are less experienced or well-

286. Trope, *supra* note 38 at 770. "The crucial element that we refer to here as the "Hurricane Sandy" test–the tendency for customers, regulators, governments, and the media to judge electric power companies by their readiness to manage an orderly and reasonably prompt restoration of service to customers." *Id.*

287. Nathan D. Taylor & Adam J. Fleisher, *Risky Business: FTC Signals Departure From Risk-Based Approach, Proposing NYDFS-Like Security Requirements for the Safeguards Rule*, MORRISON FOERSTER (Mar. 13, 2019), https://www.mofo.com/resources/publications/190313-proposing-security-requirements-safeguards-rule.html?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original.

288. *Id.*

289. *Id.*

290. *Id.*

291. *Id.*

292. Taylor & Fleisher, *supra* note 287.

293. *Id.*

resourced. Stakeholders should seize this opportunity, before political pressure and reactive legislation arrives, to take the lead and proactively drive activity in response to high-impact cyber-events. Reactive approaches often result in "ineffective polic[ies] that focus[] more on inconsequential compliance than actual protection."[294] Instead, we must "treat the threats as serious and potentially imminent, because once they prove to be, it will be too late to make the necessary preparations."[295] Rather than potential adversarial standoffs between regulators and the regulated, now is the time to collaborate and improve security across the board.[296]

VI. CONCLUSION

Utility regulators and utilities share a common goal of achieving a cost effective fully operational and safe environment.[297] Regulators want to assure utilities are able to serve their customers consistently and satisfactorily.[298] And Utilities recognize that regulators must have a process for approving a reasonable rate of return on the cybersecurity investments by those utilities and conducting periodic audits of those expenditures as well as security implementations.[299]

A disruption of that balance by a utility's assumption of unnecessary risk is counterproductive for all. The decisions of unregulated utilities, e.g., municipals, and co-operatives, have different drivers. Stakeholders should continue exploring how those decisions are made and how they might impact the overall security of the grid. Ultimately, all utilities want to avoid being in the news for having their operational environments compromised by unauthorized actors and having to explain why that was able to happen in the first place.[300]

Contrary to some arguments or assumptions, utilities and regulators do not have diametrically opposed and conflicting interests. While methods and motivations may differ, under the regulatory compact, delivery of safe and reliable service at a reasonable price is a shared goal, regardless of differences of opinions on the appropriate approach.[301]

The focus on risk-based approaches to cybersecurity has largely developed under the fast-moving free market models that technology companies operate on.[302] Those markets would ideally allow the latest, best, most popular technology, or service win.

What makes utility services different is that, in other technology sectors, people typically have a choice as to what other services they choose to purchase

294. Laughlin, *supra* note 104, at 362.
295. Trope, *supra* note 38, at 779.
296. Hellman, *supra* note 130, at 173.
297. *Id.*
298. *Id.* at 173-74.
299. *Id.* at 174.
300. *Id.* at 177-78.
301. Hellman, *supra* note 130, at 173-74.
302. *Id.* at 174.

and what associated risks they are willing to take. For example: if a consumer is unhappy with Starwood/Marriott, the consumer can stay at countless other branded hotels. The practicable service options for utility consumers is significantly more constrained.

If a consumer is hesitant to shop at Home Depot or Target, the consumer can visit Lowe's or Walmart. If a consumer is, on the other hand, unhappy with the local utility's cybersecurity practices, there is little choice other than moving or undertaking the costly and arguably inefficient task of going "off-the-grid" with self-sufficient utility services.

The question is, can consumers expect a certain level of minimum cybersecurity maturity from the utility, no matter the size or location? Furthermore, can peer utilities and others in the sector expect a certain level of cybersecurity maturity and sophistication from entities that are electrically, operationally, financially, and by reputation interconnected to them?

There is both a place for minimum standards, and the room for additional creative excellence. Government and industry have different areas of expertise in national defense, energy policy, technology deployment, and grid operations. It would be a mistake not to leverage those competencies in a complementary manner to improve overall security.

Large utility sector entities have typically established mature and sophisticated risk-based cyber defense postures while also allocating resources toward adherence with government-initiated and required compliance-based frameworks.[303] Smaller entities, with limited resources may struggle to achieve the same level of defense posture.

Once a large-scale disruptive event occurs, it may be too late to proactively shape the resulting regulatory scheme that will inevitably be imposed. Security is a team sport, and what happens to one of us happens to all of us. Legislative reactions and overreactions, reputational damage, operational damage, and financial damage inevitably cascade throughout the industry. The industry has an opportunity to lead the conversation to develop sensible requirements and assure a continued partnership between government and companies in different sectors.

303. *Id.* at 175.