Best Practices for Shared Responsibility Among Technology Platforms:

ADOPTING THE LESSONS AND PERSPECTIVES OF CRITICAL INFRASTRUCTURE INDUSTRIES

Kiersten E. Todt[1]

November 2019

DATA Catalyst

ABSTRACT

Over the past 20 years, a growing number of large technology companies have become part of the "critical infrastructure" of the United States. Given that these platforms are now essential to U.S. economic and national security, they have an obligation to collaborate with the federal government to promote security, while maintaining flexibility to support continued innovation. One approach for doing so is called "shared responsibility" (also labeled "self-governance" and "self-regulation"). Existing shared responsibility frameworks and standards for protecting infrastructure, such as the National Institute of Standards and Technology Voluntary Cybersecurity Framework, can serve as a model for these technology platforms, with adoption of several "good practices" that are tied to these frameworks and actions that reflect the need for invention and innovation beyond models that already exist. Looking forward, technology platforms should organize as a sector to create a consortium and develop robust common standards, which will help them develop an effective relationship with the public sector and create viable solutions to pressing challenges.

INTRODUCTION

One of the most noteworthy developments of the past two decades has been the rapid emergence of technology companies such as Facebook, Google, Twitter, Amazon, Uber, and others. Most of them have achieved significant market share and profitability. In the process, they have become woven into the fabric of everyday life for hundreds of millions of people in the United States and billions of people throughout the world.

The prominence of such companies, in addition to how their technologies are being used, have made them part of a new infrastructure sector that has become a cornerstone of U.S. economic and national security. As such, it is incumbent upon the companies within this sector to act with the responsibility and accountability expected from other sectors that are critical to the country's security, health, and well-being. Robust collaboration between government and this emerging sector is required to craft a successful approach that promotes security while also preserving enough flexibility to support innovation. "Shared responsibility" (which can also be labeled "self-governance" or "self-regulation") is part of the solution; but it is not the complete solution.

THE IMPERATIVE OF DATA PRIVACY AND PROTECTION

Data privacy and protection should be priorities for every business, large or small, regardless of sector or geographic location. Data collection has become a critical component of all business operations, whether it is the collection of client data to perform a simple service, or collection of enterprise data to ensure the operations of critical infrastructure. In today's operating environment, and with the continued expansion of the digital economy, data is a critical asset of every company.

Despite the functionality and importance of data, businesses rarely invest in robust data protection tools.[2] This has led to calls for the U.S. government to enact regulations that would require companies to maintain such tools, but regulation should not be treated as the only potential solution. For example, in 2016 the independent, bipartisan Commission on Enhancing National Cybersecurity recommended a market-based approach to securing Internet of Things (IoT) devices. This recommendation reflected the growing interdependencies among these devices, which typical regulatory approaches that focus on single organizations, actors, and components struggle to address. Market forces, said the Commission, would create incentives for companies to secure IoT devices, which meant that companies would define their business case for why "secure to market" should trump "first to market." If those market forces fail and companies do not take appropriate steps to secure IoT devices, then regulation should be introduced.[3]

Ideally, a market-focused strategy would be the foundation for protecting today's digital economy, which is underpinned by a global, interdependent digital infrastructure that poses increasingly complex and difficult security challenges. A primary obstacle is determining how to evolve a security strategy that aligns with today's technology and innovation. Because traditional security models have physical components at their core, those models miss many of the elements of digital threats to the country's critical infrastructure. Digital infrastructure and interdependencies that increasingly define the economy and threat environment create new challenges, like privacy, that require new thinking and new approaches.

Prominent thought leaders have suggested industry shared responsibility[4] as an appropriate path forward for technology platforms. For example, Balkin and Zittrain have advocated for an information fiduciary approach that would create structures to ensure technology platforms meet an obligation "to act in a trustworthy manner in the interest of another."[5]

Today, technology platforms have already integrated into and in some instances transformed the communications and transportation industries. The functions and capabilities that technology platforms provide are also being rapidly integrated across finance, energy, healthcare, and physical infrastructure systems, among others. As these technology platforms grow more central to every industry, almost all organizations and businesses are part of a value chain that connects them to critical infrastructure.[6] Plus, extraordinary amounts data are held by each of these platforms. Therefore, data privacy and protection need to be a priority for all enterprises. Before identifying effective data privacy and protection practices, it will be useful to provide background on critical infrastructure.

DEFINING CRITICAL INFRASTRUCTURE

In 1998, then-President Clinton signed a presidential decision directive focused on developing, within five years, a national capability to protect critical infrastructure from intentional disruption. The directive defined "critical infrastructure" as "those physical and cyber-based systems essential to the minimum operations of the economy and government."[7] As part of that directive, the U.S. government created categories of critical infrastructure, including telecommunications, finance, health, and energy.[8] But even as the digital economy exploded during the intervening years, U.S. security policies remained focused on traditional industries.

Modernizing that approach is long overdue, and any such modernization must reflect the deepening of infrastructure interdependencies.[9] With technology platforms holding vast reservoirs of data tied to their customers, often operating at the nexus of their customers' personal and professional lives, they have evolved into a component of critical infrastructure. (The impact of these technology platforms on elections only adds to their importance and role in the digital economy.) And yet, the definition of critical infrastructure has not evolved with the development of the digital economy. Specifically, one of the fundamental infrastructure components of the digital economy is data, but the U.S. government has not identified those companies that collect and possess data as critical infrastructure the way it defines a power grid or an interstate highway as critical infrastructure.

Ideally, given that data has become one of the world's most critical assets,[10] companies (both large and small) which hold this data should cooperate with each other and engage with government agencies to ensure it is protected and that the resources of both the public and private sector are used to protect it.

WHY TECHNOLOGY PLATFORMS QUALIFY AS BEING CRITICAL INFRASTRUCTURE

Technology platforms are aggregating personally identifiable information at rates and quantities greater than at any other time in the history of the world.[11] This information meets the definition of "critical infrastructure," given that it is the gateway to accessing systems and networks to which an individual is connected (i.e., workplace, banks, healthcare endpoints) – and these systems and networks constitute traditionally-defined "critical infrastructure." Underscoring just how "critical" these platforms are, they effectively "own" the digital identities of virtually any individual and institution that has a digital footprint.

Also highlighting the "critical" dimension of technology platforms is their role in helping to mitigate natural or man-made disasters. For example, social media aided in the response to Hurricane Sandy in 2012, Facebook became a communications tool when a 9-1-1 system went down in a county outside of Washington, DC in 2016, and the Coast Guard depended on Twitter to deliver information in the aftermath of Hurricane Maria on Puerto Rico in 2017.

Technology platforms were developed to innovate, make tasks easier, faster, and more convenient, and to create connections among people around the world. But the technologies have quickly grown to be much more than that, and technology companies should understand and address the fact that their platforms are being applied in ways well beyond what was initially intended.

Given that the technology sector meets the definition of "critical infrastructure," a major issue becomes how to most effectively protect these networks owned and operated by the private sector. But traditional approaches to protection cannot be applied absolutely. Several non-traditional approaches to protection have proved effective, however, and the most prominent of them are described below.

ADOPTING GOOD PRACTICES FROM THE SHARED RESPONSIBILITY FRAMEWORKS OF CRITICAL INFRASTRUCTURE INDUSTRIES (CII)

Given that technology platforms are critical infrastructure, what can be done to protect them? What approaches have worked to secure infrastructure following the convergence of physical and cyber systems?

Effective, shared responsibility frameworks and standards for protecting infrastructure that may serve as a model for technology platforms include the National Institute of Standards and Technology (NIST) Voluntary Cybersecurity Framework,[12] the U.S. Department of Energy's C2M2 (Cybersecurity Capability Maturity Model),[13] and the International Organization for Standardization (known as "ISO") 27001 (Information technology – Security techniques – Information security management systems – Requirements).[14] We elaborate further on these below.

Multi-Stakeholder Negotiation Process

The first good practice that technology platforms can adopt from critical infrastructure industries is the multi-stakeholder negotiation process. Under this process, the platforms set agreed frameworks and standards (such as those listed above). ISO, which is an independent, non-governmental organization founded in 1947, has a well-established process for industry to collaborate with NGO and public-sector stakeholders to establish common rules of the road, or "standards." A trusted commission of experts oversees a body of stakeholders that include representatives from the industry's ecosystem. For technology platforms, this ecosystem would include the platforms themselves, their major developers, their core customers, and additional suppliers that have bearing on the use, management, and security of data. In addition, it would include vital stakeholders such as those organizations that can speak for the interests of platform users. It would additionally include other public interest representatives from the public sector and civil society.

In this model, industry voluntarily agrees to comply with the standards that emerge from the negotiation amongst the various representatives. This approach is initiated by an industry body and creates incentives to act as a sector, similar to the American Chemistry Council Responsible Care initiative. Compliance hinges on contracting with a trusted and independent third-party to conduct an audit, or certification, to assess the depth and quality of compliance. Non-compliance is publicly reported. In its simplest form, transparency creates incentives for a company to self-enforce and take corrective action to avoid customers and other stakeholders spurning it for non-compliance. And while there is no guarantee that every company in an industry sector will participate, attracting the largest and most respected companies will signal to others that it's in their self-interest to join.

Multi-Stakeholder Negotiation Process Example

The Global Network Initiative (GNI) is an example of a multi-stakeholder group that counts technology platforms as participating members. GNI is an alliance of Internet and telecommunications companies, human rights and press freedom groups, investors, and academic institutions from around the world focused on helping companies "respect freedom of expression and privacy rights when faced with government pressure to hand over user data, remove content, or restrict communications."[15] It has played an important role in helping technology platforms negotiate terms with sovereign governments regarding what data can be shared for lawful reasons, and what must be protected.

Understanding Critical Infrastructure Frameworks and Standards

The second critical infrastructure industry good practice is the resulting elements and components of the standards and frameworks themselves. To illustrate what potential elements can look like, the Voluntary Cybersecurity Framework guides companies to manage four core elements:

1. Functions – Identify, Protect, Detect, Respond, and Recover
2. Categories – such as "Asset Management," "Identity Management and Access Control," and "Detection Processes."
3. Subcategories – these further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated."
4. Informative References – these are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory.[16]

Similarly, the U.S. Department of Energy's "C2M2" program establishes key domains and sets criteria to enable companies and their stakeholders to assess their level of progress and sophistication in managing cybersecurity. An example of this includes:

Risk Management –

1. Establish Cybersecurity Risk Management Strategy
2. Manage Cyber Security Risk
3. Management Activities.[17]

These frameworks, models, and standards merge the cultures of business and regulation and create steps that fit culturally with the approach companies take to set strategies, organizational policies, operational processes, procedures, and assessment. At the same time, the elements direct companies to make decisions that adhere to the wider public interest.

The GNI, referenced above, sets its own framework for companies to adopt. It includes:

- Principles to support (freedom of expression, privacy, responsible company decision making, multi-stakeholder collaboration, and governance/accountability/transparency)
- Implementation Guidelines that guide governance, management, accountability, and processes
- An Accountability, Policy, and Learning Framework, and
- A Governance Charter.[18]

The Voluntary Cybersecurity Framework and C2M2 are noteworthy in that companies voluntarily opted into using them. And in the case of the Framework, companies voluntarily opted to help develop and update it.

The Framework was one element of Executive Order 13636, which then-President Obama issued in 2013. It tasked a government entity with a reputation for objectivity, NIST, to manage the process. The value of the NIST process came from the government convening and facilitating industry but allowing industry to develop the Framework. Initially, many of the industries rejected the idea. But NIST convened additional workshops around the country, and during the second one, when industry saw that their comments were reflected in the revised document, momentum began to shift. These companies had to choose whether they wanted to denounce a process as worthless or contribute to it to make it worthwhile, and they became more engaged with and supportive of the initiative when they saw that their comments, efforts, and inputs were driving the content development. Ultimately, they played an essential role in shaping the Framework, which has proven to be a valuable tool to encourage best practices.

What does it mean to be identified as critical infrastructure?

A third good practice underpinning the success of these frameworks and structures was the recognition by the companies that, because they are within a sector identified as critical by the government, they are subject to the regulation of those sectors. (Note: Presidential Policy Directive 21 identifies the sectors that are critical.)[19] As part of this acknowledgement, the companies recognize that they would be subject to new regulation if they failed to implement additional protections defined by the cybersecurity frameworks above and partner with government. This is a key driver in understanding and asserting how technology platforms could follow a similar approach.

The federal government's definition of critical infrastructure evolved with the Presidential Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, which tasked the Department of Homeland Security, in coordination with Sector Specific Agencies (SSAs), to annually identify and maintain a list of critical infrastructure entities that meet the criteria specified in EO 13636, *Improving Critical Infrastructure Cybersecurity*, Section 9(a) ("Section 9 entities") utilizing a risk-based approach. Section 9 entities are defined as "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."[20]

When wrestling with the challenges of protecting data privacy and security, technology platforms may resist being designated as "critical infrastructure," given that the designation subjects them to extensive bureaucratic and regulatory requirements.[21] Companies often believe that being defined as critical infrastructure comes with substantial accountability and responsibility and without the advantages of government support. Technology platforms could also share the concern that being designated as critical will stifle their ability to innovate. The creation of the Financial Systemic Analysis and Resilience Center (FSARC) was a response on the part of the six largest banks to being defined Section 9 companies. The companies were concerned about the ability of the government to support their protection, and this concern prompted them to come together and work with government to create their own hybrid security infrastructure.

Collective Action, Responsibility, and Accountability

This third good practice, therefore, comes with an amendment, leading to the fourth good practice area. This practice is to adopt an approach to collective responsibility and accountability across industry and government, focused on anticipating and addressing critical threats and risks.

Data security threats, which include cybersecurity threats with national security implications, are too substantial and complex for self-regulation and self-governance to address alone. While it may be tempting to rely on law enforcement to prosecute individual bad actors for influence operations, this approach will do little to deter and disrupt nation-state attacks or organized malicious activity. One component of the security strategy should be a joint effort between government and technology platforms that is focused on coordinated, early-warning actions and pre-event planning. For example, the Department of Homeland Security (DHS) is currently building on its successful work with technology platforms during the 2018 election cycle by expanding the newly created Elections Infrastructure Information Sharing and Analysis Center and through the Protect 2020 initiative.

This level of coordination between government and the technology platforms represents progress. However, there is still more work to be done. The collaboration between the technology platforms and government, specifically focused on elections, should be a key part of a continuous learning cycle that supports the capacity to respond to new and evolving threats.

Recommendation

Technology platforms should create a consortium or industry association that works with government to protect the information they are gathering, to be transparent about the information they have, and to collaborate with the public sector on making our nation more secure. These companies would benefit from the engagement and input of traditional infrastructure companies, such as telecommunications, which have experienced growing pains from innovation.[22]

It behooves technology platforms to organize as a sector and define the roles and responsibilities they now have. A unified approach that's focused on pre-emptively addressing emerging challenges will strengthen their relationship with government and help create effective solutions.

The window for voluntary action is closing. As the 2020 Presidential election approaches, the federal government will be under pressure to enact new regulations. But when responding to national security threats, federal regulations often over-compensate when trying to address past vulnerabilities. When it comes to critical infrastructure, government only knows the physical world and it will use this approach to regulate the digital world, which will guarantee the least desirable outcomes for this sector.

CONCLUSIONS AND NEXT STEPS

Technology platforms are an evolution of traditional infrastructure. Therefore, strategies to secure these platforms, which impact our national and economic security, must represent that evolution and not be entrenched in historical models. Historical models should inform future action and be adapted, not imitated.

Step one is for technology platforms to organize as a sector, create a consortium, and define the roles and responsibilities they now have. They must be more transparent about the information they collect. If these companies can develop robust common standards, they will be better positioned to develop an effective relationship with the public sector and create viable solutions. If they don't, government is more likely to come in with a regulatory hammer, rather than a scalpel, with actions that will impede the ability of these platforms to continue to grow and innovate. An example of such an action could be breaking up of these platforms into multiple, smaller entities.

Once this consortium is established, step two is for these companies to coordinate and collaborate with government on early-warning detection and activities and pre-event planning, as well as response and recovery. Specifically, technology platforms should work with government, pre-event, to understand nation-state activity and threats which government knows more about than industry. Industry can in turn share the intelligence it has gathered on its platforms; government and industry can then coordinate their information to develop appropriate protection, prevention, resilience, and response protocols. Technology platforms would also benefit from engaging with traditional infrastructure companies, such as telecommunications, that have weathered the regulatory process for many years. While these steps will not relieve companies of the need to address existing challenges (such as data breaches), they will help prevent such breaches and help mitigate the harms associated with them.

Technology platform companies should coordinate with the federal government to develop approaches to protecting data, privacy, and the infrastructure upon which our national and economic security depends. Such collaboration would ensure that innovation is supported rather than suffocated, and that the country's national and economic security interests are prioritized in the public and private sectors.

ENDNOTES

[1] Kiersten E. Todt is the President and Managing Partner of Liberty Group Ventures, LLC and the Managing Director of the Cyber Readiness Institute. She is also the Resident Scholar in Washington, DC of the University of Pittsburgh's Institute for Cyber Law, Policy, and Security. She most recently served as executive director of the Presidential Commission on Enhancing National Cybersecurity.

[2] The EU's General Data Protection Regulation (GDPR) has brought this under-investment to light. See https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/GDPR%20compliance%20after%20May%202018%20A%20continuing%20challenge/GDPR-compliance-after-May-2018_A-continuing-challenge.ashx

[3] Commission on Enhancing National Cybersecurity, "Report on the Securing and Growing of the Digital Economy." NIST. December 1, 2016. https://www.nist.gov/system/files/documents/2017/01/19/commission_public_meeting_november_21_2016_clean_final.pdf

[4] This strategy has an extensive and well-documented history. Industry-led models, such as the American Chemistry Council's Responsible Care initiative, require members to adhere to a set of self-determined policies and practices regarding their commitment to protect health, safety, and environmental well-being. Similarly, the Forest Stewardship Council is a multi-stakeholder version, with industry negotiating with civil society to define and certify standards of sustainable forestry. These types of sector initiatives are typically required for membership in the sector organizations in order to incentivize use of industry-accepted best practices. For example, enrollment in the Responsible Care initiative is a condition of American Chemistry Council membership.

[5] Jack Balkin and Jonathan Zittrain, "A Grand Bargain to Make Tech Companies Trustworthy." The Atlantic. October 3, 2016. https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/

[6] Thomas Poppensieker and Rolf Riemenschnitter, "A new posture for cybersecurity in a networked world." McKinsey. March 2018. https://www.mckinsey.com/business-functions/risk/our-insights/a-new-posture-for-cybersecurity-in-a-networked-world

[7] https://fas.org/irp/offdocs/pdd/pdd-63.htm

[8] See John Moteff and Paul Parfomak, "Critical Infrastructure and Key Assets: Definition and Identification." Congressional Research Service. October 1, 2004. https://fas.org/sgp/crs/RL32631.pdf

[9] A Report from Argonne National Laboratory notes that "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, the 2013 National Infrastructure Protection Plan, and the Voluntary Private Sector Preparedness Program highlight the need for owners and operators to consider dependencies and interdependencies that exist among critical infrastructure systems and how they affect business continuity, security, and resilience management…Enhancing the protection and resilience of U.S. infrastructure is an urgent goal—a goal made more challenging by the inherent dependencies and interdependencies within infrastructure systems. Dependencies and interdependencies influence all components of risk (threat/hazard, vulnerability, resilience, and consequence), can themselves be a threat or hazard, affect the resilience and protection performance of critical infrastructure, and lead to cascading and escalating failures." See, Frédéric Petit, Duane Verner, William Buehring, David Dickinson, Karen Guziel, Rebecca Haffenden, Julia Phillips, and James Peerenboom, "Analysis of Critical Infrastructure Dependencies and Interdependencies." Argonne National Laboratory. June 2015. P. ix, 1. https://publications.anl.gov/anlpubs/2015/06/111906.pdf

[10] "The world's most valuable resource is no longer oil, but data." The Economist. May 6, 2017. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

[11] See for example the analysis in Darrell M. West and John R. Allen, "How artificial intelligence is transforming the world." Brookings. April 24, 2018. https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world/

[12] https://www.nist.gov/cyberframework/framework

[13] https://energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf

[14] https://www.iso.org/standard/54534.html

[15] https://globalnetworkinitiative.org/

[16] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf, p. 7.

[17] https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf. P. 22.

[18] https://globalnetworkinitiative.org/core-commitments/

[19] https://www.dhs.gov/cisa/critical-infrastructure-sectors

[20] Presidential Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure Support to Critical Infrastructure at Greatest Risk ("Section 9 Report") Summary, May 8, 2018.

[21] See Moteff and Parfomak, (2004).

[22] Historically, large technology companies (such as Microsoft and IBM) that have ignored legitimate government concerns about outsized influence often are the target of a government lawsuit.