Internet Infrastructure Risk Economics Research Issue Brief

2019

Prepared by:

Erin Kenneally, Program Manager
Cyber Risk Economics (CYRIE)
DHS Science & Technology

David Balenson, Ashley Begley, Christina Davis, and Lucien Randazzese
SRI International

INTRODUCTION

Recent incidents have exposed infrastructure vulnerabilities that have resulted in widespread service interruptions. For example, service disruptions with YouTube, Gmail, and Snapchat stemmed from Google Cloud misconfigurations and software bugs,[1] while internet infrastructure firms and web security companies recently experienced significant outages due to Border Gateway Protocol (BGP) rerouting issues with a major internet service provider (ISP).[2] Arguably more perilous was the exploitation of a Microsoft operating system (OS) vulnerability in the spring of 2017 by WannaCry, which infected more than 300,000 systems in 150 countries and crippled England's National Health Service, Spanish mobile provider Telefonica, and German railway operator Deutsche-Bahn, among other critical infrastructures.[3] The confluence of these incidents and myriad other "events" should lead to paramount questions such as: who is responsible for understanding cyber exposures that span sectors, dispersed geographies, and cross supply and value chains? What is the threshold of negative impact that should motivate stakeholder collective action in measuring and modeling exposures, or will we keep normalizing and accepting cyber risk information asymmetries? Do we have enough ground truth to inform mechanisms to incentivize and enforce preemptive, preventative controls and resiliency?

The U.S. domestic and global economies, and much of their supporting critical infrastructure, are dependent on the internet. While this may seem obvious, public and private sector decisionmakers and defenders are challenged to understand the internet's vulnerabilities, as well as the natural and manmade threats faced by the internet. These entities also struggle to capture and quantify the likelihood and impact that vulnerabilities and threats to the internet have on the security, stability, and resilience of dependent critical infrastructure, such as power grids, water supplies, communications systems, and financial networks.

This issue brief focuses on raising awareness of the state of affairs regarding internet infrastructure risk assessment and related supply chain accountability. In particular, the brief highlights the role of research and development (R&D) in identifying and understanding the existing and emerging vulnerabilities and threats to internet infrastructure to inform effective internet infrastructure risk management.

Internet infrastructure is a confluence of physical and logical functions and communication resources (e.g., data centers, exchange facilities, transmission lines and access services, software and connection services, traffic routing protocols and equipment) that enable internet usage and are owned, controlled, and coordinated through a distributed network of private and public sector entities. Internet infrastructure risk comprises the vulnerabilities and threats endangering internet infrastructure functions and resources. These vulnerabilities and threats can have consequential impact for entities within supply chains, as well as individuals and organizations who rely on internet communications to conduct their lives and business. Threats to internet infrastructure include intentional physical attacks and electronic disruptions (e.g., data interception, service hijacking), environmental

[1] Barrett, Brian. "The Catch-22 That Broke the Internet." *Wired*, June 7, 2019. https://www.wired.com/story/google-cloud-outage-catch-22.

[2] Hay Newman, Lily. "The Infrastructure Mess Causing Countless Internet Outages." *Wired*, June 28, 2019. https://www.wired.com/story/bgp-route-leak-internet-outage/amp.

[3] Rosenblatt, Seth, "Critical Systems at the heart of WannaCry's impact." *The Parallax*. May 19, 2017. https://the-parallax.com/2017/05/19/critical-systems-wannacry-impact/.

and natural disasters (e.g., hurricanes, floods), and accidental technical failures and malfunctions (e.g., human factors, power surges).[4]

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Cyber Risk Economics (CYRIE) Program supports applied R&D that addresses the business, legal, technical, and behavioral aspects of the economics of cyber threats, vulnerabilities, and controls.[5] The Stakeholder Exchange Meeting (SEM), a semi-annual DHS S&T event, convenes key stakeholders, technologists, and researchers from industry, government, and academia to discuss cyber risk economics research gaps, challenges, and opportunities. The theme of the April 2019 SEM was "Internet Infrastructure Risk Economics," and the discussion focused on the incentives that drive organizational decisions and the behaviors affecting internet infrastructure exposures. This brief is based primarily on SEM stakeholder input and supplemented by information from the CYRIE Capability Gaps Research Strategy.[6] This brief is not intended as a comprehensive or guiding policy document; rather, it highlights some recurring internet infrastructure risk pain points and illuminates how applied research and advanced development can help to close the knowledge and action gaps related to internet infrastructure risk management.

INTERNET INFRASTRUCTURE RISK ASSESSMENT

Organizational leaders' lack of understanding and effective assessment of cyber risk remains a fundamental challenge in cybersecurity, and internet infrastructure is no exception. The limited understanding of how risk is correlated across the internet infrastructure ecosystem makes it difficult to clearly identify concentrations (and diversity) of risk and determine the impact of controls on risk outcomes in dynamic threat environments. Without empirical data, it is difficult to develop, test, and apply models and methods that accurately quantify risk in a sustainable and scalable manner. Notable pain points include:

- Internet infrastructure owners and operators lack interoperable tools for systemic risk assessment. ISPs have insufficient information about the nature, magnitude, and likelihood of the risks facing their infrastructure and associated critical infrastructure networks, a condition exacerbated by the low frequency and dynamism of systemic risk incidents.
- At an entity level, it is difficult to measure the intent and identify the source of internet infrastructure risk (i.e., to differentiate between adversarial, environmental, or accidental sources of risk).
- Current legal frameworks are either ill-suited or inconsistently applied when it comes to adequately assigning responsibility or allocating costs for internet infrastructure incidents; this contributes to the lack of incentives for organizations to invest in sufficient cybersecurity controls, engage established risk mitigation frameworks, or support innovative approaches to reducing exposures.

[4] Based on terminology used in the 2015 European Union Agency for Network and Information Security Threat Landscape and Good Practice Guide for Internet Infrastructure. https://www.enisa.europa.eu/publications/iitl/at_download/fullReport.

[5] DHS S&T Cyber Risk Economics Program. https://www.dhs.gov/science-and-technology/cyrie.

[6] DHS S&T Cyber Risk Economics Capability Gaps Research Strategy. 2018. https://www.dhs.gov/publication/cyrie-capability-gaps-research-strategy.

Moreover, the role for R&D has been underserved against the backdrop of dispersed operational control, shared risk, and ambiguous responsibility for internet infrastructure security. As a result, data and analytical gaps have become a self-perpetuating cycle of underachieving production and inadequate sharing of risk measurements and metrics, as well as incomplete model testing and evaluation. The April 2019 SEM showcased some of the bellwether research aimed at closing these gaps and illuminating the value of R&D for internet infrastructure risk:

- John Heidemann, Principal Scientist, Information Sciences Institute, University of Southern California, has developed an internet outage detection capability that identifies all outages longer than 11 minutes.[7] This tool uses active measurement techniques and statistical models to estimate the reliability of networks as a whole and identify the portions of a network that are less reliable. With near real-time reporting as well as a dashboard of the data, events are reported within two hours of occurrence, visualized on a world map, and will soon be accessible via a data streaming API.[8]
- Alberto Dainotti, Research Scientist, Center for Applied internet Data Analysis (CAIDA), summarized CAIDA's internet outage and cybersecurity metrics projects that enable critical communication infrastructure decision analytics, with a focus on the risks and impacts of incidents.[9] CAIDA is also developing techniques to measure and predict how attackers can affect a country's centralized internet traffic transit points and hijack internet traffic.

Notably, both research teams provision their data, models, and tools to the broader cybersecurity community via the Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT),[10] a unique resource that operationalizes information sharing to close data and knowledge gaps across various cybersecurity challenge problem areas, including internet infrastructure security.

Research Opportunities

The SEM discussion highlighted the following focus areas for risk assessment research that can appreciably impact internet infrastructure risk management:

- Development of methods to differentiate between types of threats and threat actors to aid in situational awareness, threat modeling, and decision support.
- Evaluation of existing metrics and development of new metrics for robust, consensus-based measurement and modeling of internet infrastructure risk.
- Development and evaluation of novel resiliency measures, especially in contexts/geographies with less redundancy built into their internet infrastructure, such as rural areas.
- Comparative modeling and evaluation of incentives mechanisms from aviation, environment, and defense safety and security domains to improve internet infrastructure security.
- Experiments to gauge efficacy of information technology (IT) security controls for shared services and functions, including the development of

[7] The ANT Lab: Analysis of Network Traffic. 2019. *Information Sciences Institute, University of Southern California.* https://ant.isi.edu.

[8] Lin Quan, John Heidemann, and Yuri Pradkin. "Trinocular: Understanding Internet Reliability Through Adaptive Probing." 2013. *Information Sciences Institute, University of Southern California.* https://www.isi.edu/~johnh/PAPERS/Quan13c.pdf.

[9] CAIDA Internet Outage Detection and Analysis. 2019. https://ioda.caida.org; Center for Applied Internet Data Analysis, University of California San Diego. http://www.caida.org/home.

[10] IMPACT Cyber Trust. https://www.ImpactCyberTrust.org; DHS S&T IMPACT. https://www.dhs.gov/science-and-technology/cybersecurity-impact.

user-friendly tools that correlate threats to controls to outcomes across systems.
- Techniques for mapping cross-enterprise and inter-industry dependencies to better understand correlated exposures, concentration of risk, and data gaps.

Potential Research Impact

Incentives for investments in internet infrastructure network security improvements and upgrades—whether via regulation, liability, insurance, or market forces—are likely to be stronger in environments with improved risk measurement and modeling capabilities. Empirical data and measurements can help inform more effective modeling of current and future sources of internet infrastructure risk. Entity- and system-level risk assessments in conjunction with controls performance measures are essential to addressing internet infrastructure risk management. Systemic risk, however, is neither easy to isolate nor amenable to traditional risk management approaches. Furthermore, causal relationships, feedback loops, and tipping points are not easily measured by segregated stakeholders, contributing to the opacity and complexity of internet infrastructure risk.[11] Solution interventions for this type of collective risk are perfectly suited for pre-competitive R&D, particularly in light of so many open questions and an uncertain market demand.

Supply Chain Accountability

The increasing complexity of supply chains and lack of optics into supplier relationships and dependencies are a major contributor to internet infrastructure risk. Most current internet infrastructure research (outside of theoretical modeling) focuses on topics for which data are readily available. Accordingly, the R&D community generally does not conduct empirical research into supply chain dynamics. This has contributed to a poor understanding of who is accountable for the harmful impacts of insecure products and practices among manufacturers, service providers, developers, and/or integrators. While the Federal Acquisition Authorities[12] serves as a model for holding government industry partners to account for meeting cyber security standards, accountability methods such as contract procurement and flow down requirements within industry supply chains are not broadly implemented enough to prevent destabilization of the internet infrastructure and the resulting broadscale risk to individuals and organizations. There are several potential mechanisms to address the accountability gap, including market-based incentives (e.g., tax credits, a robust cyber insurance market, procurement standards) and regulation (e.g., equipment certification, breach disclosure requirements, software component disclosure). The following factors hinder accountability improvements:

- Component and system manufacturers lack standardized techniques to measure cyber risks induced by third-party supplied technologies.
- Available data on specific targets in a supply chain network (e.g., chips, boards, software libraries, applications, etc.) are limited in scope and scale.
- Dependencies within and across supply chains are difficult to map because of information asymmetries, which increases the chance of a systemic

[11] See, e.g., International Risk Governance Council (IRGC). “Guidelines for the Governance of Systemic Risks.” 2018. *Lausanne, Switzerland: IRGC.* https://infoscience.epfl.ch/record/257279/files/IRGC%20Guidelines%20for%20the%20Governance%20of%20Systemic %20Risks.pdf.

[12] See, e.g., "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.” NIST SP 800-171 Rev. 1. December 2016. https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final.

failure of significant portions of the supply chain.

The April 2019 SEM included the following stakeholders' perspectives about internet infrastructure risk and supply chain accountability:

- Morgan Hervé-Mignucci, Director, Cyber Risk Modeling, CyberCube, focuses on cyber risk modeling of cyber insurance.[13] He stressed the need to complement available measurements on cyber risk hygiene in order to prevent over-interpreting available data or drawing conclusions from over-simplified models. Proposed solutions include network-facing internal assets, extended IT, essential/critical services, and generalizable vendor roles.
- Suresh Krishnaswamy, Senior Engineer and Principal Investigator, Parsons Corporation, is pursuing enterprise-level internet exposure risk (IER) scoring based on multi-dimensional measures of the interdependencies between organizations' information systems.[14] The benefits of this approach include: enabling stakeholders to gauge the level of exposure to loss events even when operators control only a subset of their organizational information systems; providing quantitative measures to support IER scores and their aggregation across a collection of enterprises; and identifying effective courses of action to mitigate their risk exposure to adverse events that target interdependencies in enterprise information system services.
- Allan Friedman, Director of Cybersecurity Initiatives, National Telecommunications and Information Administration (NTIA), and his team are working with industry to design and implement a Software Bill of Materials (SBOM) for third-party components and software.[15] Analogous to a list of ingredients on food packaging, SBOM would extend the well-established practice in traditional manufacturing as part of supply chain management to include a list of components in a piece of software. Buyers could use a SBOM to ensure software components are up to date, evaluate product risk, and respond quickly to newly discovered vulnerabilities.

Research Opportunities

The SEM discussion highlighted the following research focus areas that can inform policy and actions by industry and government to advance supply chain accountability:

- A better understanding of data gaps and limitations, including missing supply chain data, lack of data origin information, and data scrubbing techniques that decrease data utility.
- Methods to quantify the nature and scope of loss from supply chain attacks at both the macro and micro levels.
- User-friendly, supply chain-focused tools and techniques that can be used by organizations to gather internet infrastructure risk data.

Potential Research Impact

A supply chain is only as strong as its weakest link, and the cascading impacts of cyberattacks can have severe consequences for downstream organizations within the same supply chain. The 2017 NotPetya cyberattack is an example of how a compromised third-party software update was used to spread malware that disrupted a

[13] CyberCube Analytics. 2019. https://www.cybcube.com.

[14] IMPACT Performers. 2019. https://www.impactcybertrust.org/who_performers; See, e.g., IMPACT Parsons Dataset. https://www.impactcybertrust.org/dataset_view?idDataset=1168.

[15] NTIA Software Component Transparency. 2019. https://www.ntia.doc.gov/SoftwareTransparency; https://www.ntia.doc.gov/blog/2019/progress-software-component-transparency.

global shipping company's operations, resulting in an estimated $300 million in damages.[16] Supply chain security research supports the development of approaches for improving security accountability within complex supply chains, as well as tools for efficient and systematic collection of cyber environmental data.

To better prepare for supply chain attacks, SEM participants highlighted the potential impact of additional research into supply chain security to improve internet infrastructure risk management:

- Robust IT and non-IT supply chain mapping can uncover unknown vulnerabilities, as current supply chain mapping often lacks IT network-layer detail and does not adequately identify potential adversary targets.
- Supply chain risk cost-benefit models can be used to incentivize organizations of all sizes to embrace their responsibility in the context of larger infrastructure risk.
- Knowledge of internet infrastructure risk exposure can be applied to cyber insurance for improved risk transfer capacity, including mechanisms for companies to share risk data and information without compromising enterprise-specific sensitivities.

NEXT STEPS

SEM participants recommended enhanced measurement, collaboration, and data sharing to inform improved modeling as themes to address internet infrastructure risk. Researchers should continue data collection efforts related to internet infrastructure to inform resilience, reliability, security, supply chain accountability, and disaster planning. Importantly, it is critical that industry and government work with research stakeholders to enhance access to empirical data and ensure that their capability requirements help guide research pursuits.

In summary, SEM participants suggested the following steps forward to improve internet infrastructure risk management:

- Develop integrated, scalable approaches to mitigate internet infrastructure risk at both the entity and system levels.
- Create spaces for ongoing communications between researchers, ISPs, industry, and government to form collaborative internet infrastructure research partnerships on data sharing agreements and platforms, metrics, and outage measurements.
- Improve quantification of risk and supply chain data collection techniques (e.g., partnerships, data clearinghouses, open-source initiatives, fundamental R&D funded with public funds, safe harbor provisions for taking measurements), with the realization that an impact on an organization's bottom line will likely be required for entities to share more data.
- Increase incentives to encourage risk mitigation efforts and data sharing across government, academia, and industry.
- Link internet infrastructure data with models to better understand the data and assess future implications of internet infrastructure risk.

[16] Greenberg, Andy. "The Untold Story of NotPetya: The Most Devastating Cyberattack in History." *Wired,* August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world.

ONLINE
scitech.dhs.gov

EMAIL
SandT.PCS@hq.dhs.gov

TWITTER
@dhsscitech

LINKEDIN
dhsscitech

FACEBOOK
Facebook.com/dhsscitech

YOUTUBE
www.youtube.com/dhsscitech

PERISCOPE
@dhsscitech

DOI: 10.23721/1504274

Recommended citation: Kenneally, Erin, David Balenson, Ashley Begley, Christina Davis, and Lucien Randazzese. "Internet Infrastructure Risk Economics Research Issue Brief". *U.S. Department of Homeland Security*, Science & Technology Directorate, September 2019, https://www.dhs.gov/science-and-technology/cyrie/. doi: 10.23721/1504274.