The Challenge of Assessing Strategic Cyber Security Risk in Organizations and Critical Infrastructure

Charles Harry, PhD

Associate Research Professor
School of Public Policy
University of Maryland, College Park

Abstract:

The increasing threat of cyber-attacks against systemically important institutions and critical infrastructure continues to highlight the need to improve the defense and resilience of organizations. The US government focuses its defense strategy on applying a risk-based approach to optimize the allocation of scarce resources across federal networks and promotion of best practice for critical infrastructure. This paper discusses the framing national policy and the core methodological challenges facing practitioners who seek to implement such an approach. The paper defines three key areas of fundamental challenge: (1) defining tiers, categories, and severity measures of end effect, (2) linkage of devices to organizational processes, and finally (3) a mechanism for connecting organizations together to analyze emergent societal effects. This approach is broadly applied to an example of commercial airline operations identifying the interconnection between key functions in the production chain, which if disrupted lead to strategic effects in the critical infrastructure sector.

Key Words: Risk, Critical Infrastructure, Cyber Strategy, Interdependence

Introduction:

The volume and severity of cyber-attacks remains an enduring challenge to industry and governments. The increasing loss of sensitive data and potential for disruption to key business processes and public services have focused senior leadership on the need to identify specific areas of organizational risk to effectively allocate resources.

This article discusses the framing national policy that adopts a risk centric approach and highlights the core methodological challenges currently facing practitioners who attempt to adopt security frameworks. Often the inability to adequately capture the inherent complexity of technology, vulnerability, and human processes leave private sector leaders unable to optimize defenses and public officials unable to deeply, and with greater nuisance, assess societal risk stemming from cascading consequence of a cyber event in critical infrastructure.

Articulating a Strategic Approach

A risk-based approach to cyber security defense is at the heart of U.S public efforts to secure federal networks and promote resilience in critical infrastructure. It is also increasingly seen as best practice across the private sector as a means of lowering the potential disruptive effects of certain types of attacks or in the safeguard of intellectual property and customer data.[1]

The US 2018 National Cybersecurity Strategy articulates four main pillars of action, specifically highlighting defense in two key areas: protecting federal networks and promoting the defense of critical infrastructure. [2] Much of this view is also supported by the recently released US Cyberspace Solarium Commission report, a bi-partisan effort focused on further refining future efforts to promote broader protection from cyber-attacks by denying benefits to threat actors as part of a concept of layered deterrence.[3] Reducing benefits to threat actors is focused on optimizing resources in the defense in key areas of importance that broadly align with the administration's strategic efforts.

First, the US government emphasizes a risk based approach in the defense of federal networks, mandating the need for department Chief Information Officers (CIO) to align IT investments with their assessment of mission risk.[4] The change in approach now directly holds agency and department leaders accountable for the defense of their networks which support critical services. Executive branch guidance serves to complement existing federal requirements that require compliance among agencies and departments within several activity areas defined in the E-Government Act of 2002[5] with updated guidance found in the Federal Information Security Modernization Act (FISMA) of 2014.[6]

US strategy also highlights the needs to align risk based approaches in the defense of US critical infrastructure, noting "The Administration will develop a comprehensive understanding of national risk ...."[7] With over 85% of the nation's critical infrastructure owned and operated by the private sector[8], the US government has emphasized the need to collaborate with industry to ensure a broader level of protection for essential services against a growing volume and severity of cyber-attacks. Recent attacks against Supervisory Control and Data Acquisition (SCADA) systems including compromise of systems in Saudi Arabian energy infrastructure[9] and the notification of a gas pipeline disruption by the Cyber and Infrastructure Security Agency (CISA)[10] emphasize the growing threat cyber-attacks represent. The Trump administration adopts existing definitions and sector assignment, [11] but expands broadly in two key areas. First, the administration uniformly adopts a more centralized and uniform approach to cyber security across the executive branch.[12] Second, the administration expands the use of specific security frameworks that seek to improve the defense of critical systems from cyber-attack.[13]

To implement risk assessment and management programs both for federal networks as well as critical infrastructure, government agencies and departments are required by executive order[14] to align with the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF)[15]. The NIST CSF serves as broad guidance aligned within five key functional areas: Identify, Protect, Detect, Respond, and Recover. Within the Identify function, the NIST CSF identifies Risk Assessment (ID.RA) and management (ID.RM) activities as key elements in a comprehensive cyber security program.[16] Within these specific set of activities the NIST CSF adopts principles and guidance from other frameworks and security control lists such as ISACA's Control Objectives for Information Technologies (COBIT), or the International Organization for Standardization (ISO) 27000 series.

The national policies and subsequent cyber security frameworks are at the heart of public sector efforts to secure federal systems and promote greater security in critical infrastructure. They have

also increasingly become identified for use by the private sector and generally are essential guidance in developing mature security programs across industries. In one industry survey, over 84% of organizations across a range of sectors and sizes responded they use an established security framework that incorporate a risk-based approach.[17]

The Challenge of Executing a Risk Based Approach

The NIST CSF and associated documents provide general standards, guidelines, and best-practices to manage cybersecurity-related risk. [18] It provides principles for systematic risk assessment, including:

- Assess the potential consequences that could result from specific threats.
- Assess the realistic likelihood of those threats to engineer the consequences identified.
- Assess the risk by asset, function, organization, and integrated risk between firms.
- Generate scenario-based use cases for estimating risk.

Actual risk assessment practices however fall short of these principles. International standards[19] and US policy[20] often recommend assessing consequences in terms of the effects on confidentiality, integrity, or availability of data, but that is a very limited way of conceptualizing damage that can be done by a cyber-attack. Standards and best practice documents do not specify a particular methodology for risk assessment and leave both the range of consequences and the metrics for estimation to be decided on an ad hoc basis complicating the ability compare across organizations or sectors.

There have been several efforts to develop industry-wide qualitative methods such as OCTAVE,[21] and one quantitative approach, Factor Analysis of Information Risk (FAIR),[22] is used by organizations in many different sectors. Both approaches direct users to input the effects of cyber-attacks with little guidance as to how that should be calculated. Analytical tools like OCTAVE and FAIR can help users begin to assess specific, often secondary effects, but by focusing attention on the costs of compromise to *individual* devices in an organization's IT network, they ignore potentially much larger consequences of a hacker-induced effect in an *interconnected* system such as the disruption to a military communication network or the ability of a city to process court proceedings.[23]

There does not currently appear to be a method or framework to assess the emergent consequence of an attacks on a single or set of devices in an organizational network with a critical infrastructure sector as a whole. In fact, the Department of Homeland Security (DHS) explicitly identifies this as an issue noting that "We lack integrated and scalable adoption and application of systemic risk assessment, resulting in ineffective and uncoordinated application of resources for cybersecurity. ".[24] DHS cites the underlying issue noting "systemic risk assessment is beset by underlying quantitative measurement difficulties which contribute to process adoption and application challenges". The inability to link device and organizational process with possible emergent sector effects remains the crux of the problem.

Organizing a Strategic Framework

While risk centric approaches to cyber security are lauded and promoted as best practice, the methods of quantitatively assessing risk is woefully immature. The challenge in developing

suitable and readily adoptable approaches stems from (1) the lack of definition of cyber effects and methods for measuring them, (2) techniques for linking devices to organizational processes, and (3) assessing impacts within a larger interdependent system of organizations.[25] Taking the range of effect and tiers of impact (e.g device, organization, sector) into account, strategic risk is not about computing a value for a single device, but more broadly for the device, the human process it supports, and finally the emergent impact it has on interlinked systems outside of the initially targeted organization.

Building a Foundation: Categorizing and Measuring Effect

In keeping with the principles for risk assessment in the NIST Standard Framework, it is helpful to consider consequences on three levels: the IT assets that work together to support particular organizational functions, the organization as a whole, and the interconnected system or systems of which that organization is a part. The cyber risk assessment framework developed by the author and colleagues at the Center for International and Security Studies at Maryland (CISSM) differentiates between primary, secondary, and second-order effects.[26] Primary effects are the direct impacts to the target organization's data or IT-enabled operations. Cyber events can also cause secondary effects to the organization, such as the financial costs of replacing equipment damaged in an attack, labor hours to address the problem, a drop in the organization's stock price due to bad publicity from the attack, or a loss of confidence in the organization's ability to safeguard confidential data. Finally, they can cause second-order effects on individuals or organizations who rely on the targeted organization for some type of goods or services. These could include effects on the physical environment, the supply chain, or even on an individual's attitudes, preferences, or opinion deriving from the release of salacious information.

Academic research on methods for estimating and predicting the effects of cyber events tends to focus on narrowly defined questions and to use whatever data is most readily available. For example, most efforts to estimate the primary effects of disruptive cyber events have involved impacts on power grids, particularly reliability and operators' ability to manage power.[27] [28] They have also concentrated on the subset of potential attack scenarios involving the convergence of information technology (IT) and Operational Technology (OT) instead of considering a wider range of disruptive scenarios involving other types of business or mission function. This research provides some valuable insights into a category of cyber threats to critical infrastructure that is of great importance. Yet, it is difficult, if not impossible, to apply estimation methods developed for primary effects of disruptive attacks on the control systems of power grids to the vast array of other mission and business functions in different types of organizations and critical infrastructure sectors of interest to public officials and their private sector partners.

Few cyber analysts have tried to model primary effects of cyber-attacks on networks of IT assets that must work together to support organizational functions rather than treating them as isolated devices. Mussman et al. do part of what is needed.[29] They create graph models of IT devices supporting specific mission functions and discuss elements of an attack that affect severity, including length of disruption. However, they model the disruptive effects on individual devices instead of estimating impacts across a system of devices attached to a specific mission function. They also do not include a method for combining different features of an attack into a single scale that can be used to measure and compare different disruptive events. They also fail to provide a repeatable method for quantifying those impacts, which precludes generalizing their approach to a variety of organizations and networks.

Research on secondary effects over the past 15 years has involved different ways to measure the financial consequences of cyber-attacks on firms. Early efforts used publicly available financial data to assess how announced security breaches affected a company's share price[30313233] and value[3435]. Generally, this body of work has looked at publically available financial data, specifically share price, to estimate the market consequences of data breaches and some forms of disruptive cyber activity such as a distributed denial of service, but whose findings often are not useful to military planners or policy makers who are more broadly concerned on the ability to support a specific mission (e.g. communicate with troops in the field) or provide a public service (e.g. process court hearings).[363738]

Various types of second-order effects have also received attention. Researchers have assessed the macroeconomic effects to transportation networks[39] and the impact hacking of autonomous vehicles would have on traffic congestion.[40]

Ideally, efforts to measure or predict the effects of cyber events for risk assessment or other purposes should use a comprehensive framework that considers primary, secondary, and second-order effects using a standard methodology that can be applied to any type of organization or critical infrastructure sector. For example, in 2018 the NotPeyta ransomware encrypted thousands of devices at the Maersk Shipping Line.[41] The direct effects on devices in the network (e.g. loss of function) are one consequence impacting availability of specific devices. However, the primary availability problems lead to the inability to transit cargo and manage containers in yards, generating operational consequences exceeding $200 million dollars.[42] Finally, the disruption to Port of Rotterdam where the cargo management system was down, led to logistic bottlenecks throughout central Europe impacting hundreds of other companies dependent on the logistics supply chain Maersk Line helped support. So, while the impacts of the cyber-attack on Maersk Line immediately impacted the availability of thousands of devices, the effects are tiered across multiple levels ll measured in different ways.

Building a Foundation: Linking Devices to Organizational Processes

Typical risk assessments often will start with a list of devices. Cyber threat scenarios are applied to each and often an estimate of likelihood and effect are made. Subsequent risk calculations are then computed and often visualized in some manner such as in a heat map. These approaches will often provide a point estimate of risk for one type of effect, with the measurement of consequence ill-defined. This approach does not account for multiple devices working together to execute a specific mission function. For example, the ability of a airline to process incoming passengers in a terminal may not simply be tied to a single application server running the software, it includes the routers and switches needed to route the packets between the application server, and the client devices (laptop, scanners, etc) used by employees. Figure 1 illuminates that devices networked together work in a topology, which itself can be attacked in a myriad of ways (i.e Data wiper on the application server, resetting router to factory settings, or

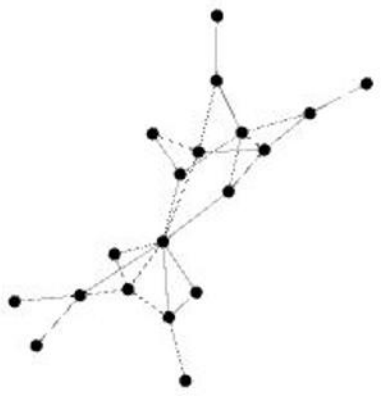

Figure 1: Devices as a Topology

ransomware on the client machines), each of which have differing vulnerabilities and consequences. With different consequences the measurement of severity will also need to change. Therefore, instead of a single measurement of consequence against a single machine, we need to account for a range of consequences against a topology which is tied to the human process it supports.

Finally, multiple processes are conducted by different departments and teams to produce a product or service. If a single process is viewed as a topology, then interlinked topologies create their own production chain. Expanding our previous example of air flight operations, an airline can check-in and board passengers, prepare an aircraft for flight, and communicate with the airport tower control to request a runway for takeoff. Therefore we need parts of our network to (1) check-in passengers, (2) we need our maintenance records system and other "Apron Handling Services" to ensure the safety of the aircraft, and (3) finally we need to communicate with the tower to allow us to take off. Linking those individual process topologies together in a representative production chain allows us to map information technology assets to the human defined production chains. If any of these processes noted in Figure 2 is impacted, a flight may not be allowed to take off. If in turn each process topology has a certain number of critical devices of which its disruption causes an inability to have the process function, then the outage of specific critical devices such as a core router or application server in customer check-in could impede overall flight operations. This very scenario occurred in 2018 when a computer tied to passenger check-in and ticketing was disrupted by a "computer outage" leading to the grounding of all Delta airline operations.[43] A similar flight disruption occurred to Southwest Airlines in 2019, when a third party venders systems went off line impeding the ability of pilots to work through flight plans.[44] In both cases different part of the production chain were impacted. For Delta, customer check in was disrupted due to the failure of technology causing a grounding of flights. In the Southwest example, "Apron Handling" services were disrupted when a 3rd party vendor's system was disrupted. In both cases failure of systems caused the grounding of flights.

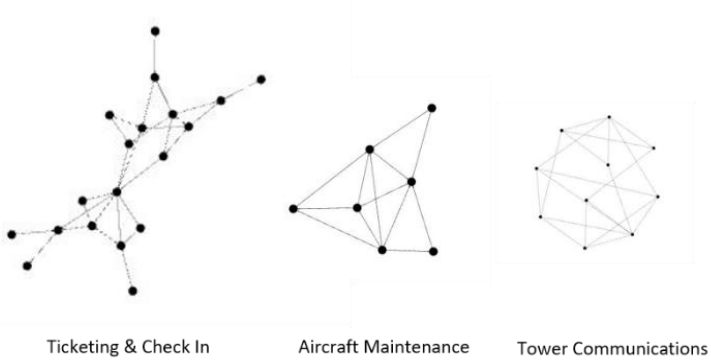

Figure 2: Production Chain of Multiple Processes

Computing risk for a complex organization cannot simply include computation of effect and likelihood for individual devices, as that ignores or at a minimum obfuscates the human processes they support. Therefore any measure of strategic effect needs start with the interconnections between devices supporting processes that link together to form a production chain. So, while one set of stakeholders, IT managers, might be concerned about the primary effects to the confidentiality, integrity, and accessibility of their devices and networks, another group, operations managers, are concerned about how those individual systems work together to support organizational operations. The loss of production, or in this case flight operations, generates lost revenue, remediation costs, brand effects, and possible legal challenges. These

consequences are measured differently than the primary effects we see on the devices themselves.

Building a Foundation: Assessing Impacts within a Larger Interdependent System

Thus far we have discussed the need to expand our definition of cyber end effects and how to associate topologies of devices to the human defined services they support. How might we consider effects on organizational services, like disrupting flight operations in single airline with the larger effects in an entire critical infrastructure? The Cyber and Infrastructure Security Agency (CISA) is focused on attempting to answer this very question by restructuring the broad question of how to defend the broad critical infrastructure categories, by defining what they term "National Critical Functions" (NCF), with the goal of pinpointing specific operations within key industries that support the public interest.[45] For example, transportation companies might broadly be lumped into the PPD-21 definition of critical infrastructure, but not all devices in the myriad of commercial airline networks are of equal importance. For example, a computer impacted with ransomware in the human resources department of a major airline, is not likely generating the same level of concern as that same ransomware impacting ticketing systems or tower communications. CISA's NCF construct focuses on the key functions that support critical societal functions such as "Transport Cargo and Passengers by Air" providing better focus to the systems that represent the greatest concern.[46]

So how do we begin to think through how devices, processes, and organizations create interdependent and emergent risk in an entire critical infrastructure? Often its useful to look at the relationships between organizations or entities where a disruption might be of concern to policy makers or industry leaders. In our example of air flight operations, we can look at a single part of the commercial airline sector. The Federal Emergency Management Agency (FEMA) divides the US into 10 regions. If we look only at data from the US Department of Transportation[47] for commercial air flights in 2019 and map the airports (vertices) and the volume of passengers (width of edges) we can visualize the interdependence of organizations in a single critical infrastructure. Figure 3 provides a map of FEMA region 10 which includes the states of Alaska, Idaho, Oregon, and Washington. The colored edges between vertices represent specific airlines. I have colored three in particular: United Airlines (Green), Sky West (Purple), and South West (Blue), with all other airlines colored grey. Vertices size is a reflection of degree (e.g number of edge connections). If any of the airports in this model were disrupted we could quantify the impact of loss flights and connections by computing the importance (e.g centrality) of the airport in the graph structure with the share of passenger flights connecting that airport with others in the

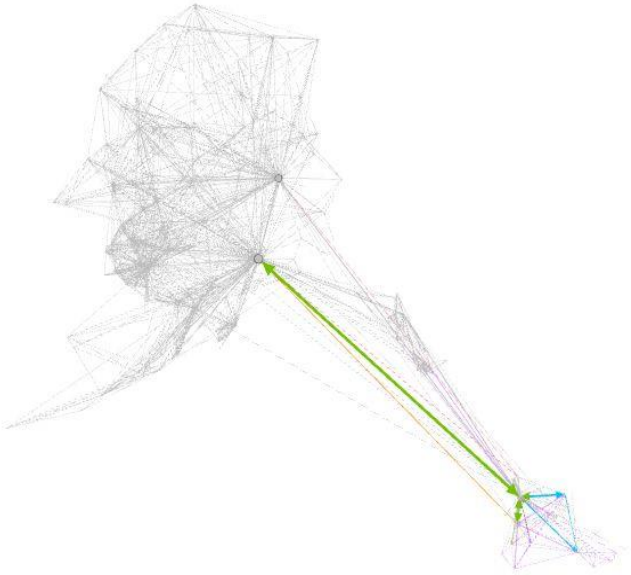

Figure 3: Commercial Air Flights in FEMA Region 10

region. If the operation of each airport is dependent upon a series of production chains executed by a combination of specific airlines and common airport infrastructure (e.g tower communications), an impact to any part of those chains can cause a disruption to a node in this organizational structure. For example, a ransomware incident in the United air ticketing system might ground all of the airline's flights. As United runs a highly significant percentage of all flights between Seattle and Anchorage, which themselves are the two most important vertices in this organizational structure, the large local effect on United's production chain translates to a potentially large strategic effect in FEMA region 10. Conversely, a ransomware attack against a small regional airline, like the attack on the RavnAir maintenance system[48] in 2019 that grounded flights, is unlikely to generate a large strategic effect given the small number of passengers they serve relative to all flights in the region.

This approach allows policy analysts and operational risk officers to identify key production chains, link processes to them and the specific devices supporting each. Attack scenarios that cause impacts to "critical" nodes (e.g. process can't function without it) cause cascading failure in the entire production chain which could lead to the loss of an entire node in the organizational map. Doing so provides a mechanism to link devices in specific airline or airport network infrastructure broader set of air flight operations provided in the region. This approach provides "connective tissue" between device (primary effect), production chain (secondary effect), and finally emergent sector level consequences (second order effect).

The Need for Methods in Measuring Strategic Risk

US national cyber policy articulates a strategy of using a risk-based approach for improving security against cyber attacks. Both the executive and legislative branches identify the ability to prioritize along these lines as a key approach to reducing the benefits to threat actors who seek to disrupt critical services and organizational networks. Yet despite the broad policy consensus, there is a dearth of quantitative methods that enable the categorization and measurement of consequences between various tiers of analysis. In fact, the inability to link device, to process, to sector remains an enduring challenge in the cybersecurity field and a current issue for assessing strategic national risk. Efforts to develop such methods including work at the University of Maryland is underway and is being applied to a range of private sector projects to identify the strategic consequences to critical infrastructures such as air transport, pipeline infrastructure, and nuclear power plants.[49] In light of the growing volume and severity of disruptive attacks, such methodological advances are necessary to judge what remains a private problem versus a broader public concern.

[1] "Trends in Security Framework Adoption", 2016, https://static.tenable.com/marketing/tenable-csf-report.pdf
[2] "National Cyber Strategy", 2018, White House, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
[3] "US Cyberspace Solarium Commission Report", 2020, US Congress, 2020, https://www.solarium.gov/
[4] "E.O. 13833: Enhancing the Effectiveness of Agency Chief Information Officers", 2018, White House, https://www.whitehouse.gov/presidential-actions/executive-order-enhancing-effectiveness-agency-chief-information-officers/
[5]"E-Government Act of 2002", PL 107-347, 2002 https://www.govinfo.gov/app/details/PLAW-107publ347/
[6] "Federal Information Security Modernization Act", PL 113-283, 2014, https://www.govinfo.gov/app/details/PLAW-107publ347/
[7] "National Cyber Strategy", 2018, White House, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
[8] "Critical Infrastructure: Long-term Trends and Drivers and Their Implications for Emergency Management", June 2011, DHS, https://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf
[9] Seals, T "SAS 2019: Triton ICS Malware Hits a Second Victim", https://threatpost.com/triton-ics-malware-second-victim/143658/
[10] "Alert (AA20-049A) https://www.us-cert.gov/ncas/alerts/aa20-049a
[11] "Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience", White House, 2013, https://www.govinfo.gov/app/details/PLAW-107publ347/
[12] "Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", White House, 2017
[13] Ibid
[14] Ibid
[15] "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1", NIST, 2016, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
[16] Ibid
[17] "Trends in Security Framework Adoption", 2016, https://static.tenable.com/marketing/tenable-csf-report.pdf
[18] The NIST Cybersecurity Framework (CSF) was released in 2014 and updated in 2018. Both versions can be found at https://www.nist.gov/cyberframework/framework.
[19] ISO 27001 "Information Security Management" https://www.iso.org/isoiec-27001-information-security.html
[20] NIST SP 800-30 Rev 1, " Guide for Conducting Risk Assessments"
[21] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419
[22] https://www.fairinstitute.org/
[23] https://www.ajc.com/news/local-govt--politics/one-atlanta-court-thousands-still-feeling-the-sting-cyberattack/xhigfzmVnnt2UTEO998C5I/
[24] "Cyber Risk Economics Capability Gaps Research Strategy", DHS, 2018, https://www.dhs.gov/sites/default/files/publications/3950_CYRIE_Report_FINAL508.pdf

[25] Harry, Charles, & Gallagher, Nancy "An Effects Centric Approach to Assessing Cybersecurity Risk, CISSM, 2019, https://cissm.umd.edu/research-impact/publications/effects-centric-approach-assessing-cybersecurity-risk
[26] Harry, Charles, and Nancy Gallagher. "Classifying Cyber Events: A Proposed Taxonomy." *Journal of Information Warfare* 17, no. 3 (2018): 17.
[27] Kundur, Deepa, Xianyong Feng, Salman Mashayekh, Shan Liu, Takis Zourntos, and Karen L. Butler-Purry. "Towards modelling the impact of cyber attacks on a smart grid." *International Journal of Security and Networks* 6, no. 1 (2011): 2-13.
[28] Stamp, Jason, Annie McIntyre, and Bryan Ricardson. "Reliability impacts from cyber attack on electric power systems." In *2009 IEEE/PES Power Systems Conference and Exposition*, pp. 1-8. IEEE, 2009.
[29] Musman, Scott, Mike Tanner, Aaron Temin, Evan Elsaesser, and Lewis Loren. "Computing the impact of cyber attacks on complex missions." In *2011 IEEE International Systems Conference*, pp. 46-51. IEEE, 2011.
[30] Campbell, Katherine, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. "The economic cost of publicly announced information security breaches: empirical evidence from the stock market." *Journal of Computer Security* 11, no. 3 (2003): 431-448.
[31] Acquisti, Alessandro, Allan Friedman, and Rahul Telang. "Is there a cost to privacy breaches? An event study." *ICIS 2006 Proceedings* (2006): 94.
[32]Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan. "The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers." *International Journal of Electronic Commerce* 9, no. 1 (2004): 70-104.
[33] Garg, Ashish, Jeffrey Curtis, and Hilary Halper. "Quantifying the financial impact of IT security breaches." *Information Management & Computer Security* 11, no. 2 (2003): 74-83.
[34] Aytes, Kregg, Steve Byers, and Mukunthan Santhanakrishnan. "The Economic Impact of Information Security Breaches: Firm Value and Intra-industry Effects." *AMCIS 2006 Proceedings* (2006): 399.
[35] Bolster, P., Pantalone, C. H., & Trahan, E. A. (2010). Security breaches and firm value. *Journal of Business Valuation and Economic Loss Analysis*, *5*(1).
[36] Hovav, Anat, and John D'Arcy. "The impact of denial-of-service attack announcements on the market value of firms." *Risk Management and Insurance Review* 6, no. 2 (2003): 97-121.
[37] Gordon, Lawrence A., Martin P. Loeb, and Lei Zhou. "The impact of information security breaches: Has there been a downward shift in costs?" *Journal of Computer Security* 19, no. 1 (2011): 33-56.
[38] Morse, Edward A., Vasant Raval, and John R. Wingender Jr. "Market price effects of data security breaches." *Information Security Journal: A Global Perspective* 20, no. 6 (2011): 263-273.
[39] Santos, Joost R., Yacov Y. Haimes, and Chenyang Lian. "A framework for linking cybersecurity metrics to the modeling of macroeconomic interdependencies." *Risk Analysis: An International Journal* 27, no. 5 (2007): 1283-1297.
[40] Vivek, Skanda, David Yanni, Peter J. Yunker, and Jesse L. Silverberg. "Cyber-physical risks of hacked Internet-connected vehicles." *arXiv preprint arXiv:1903.00059* (2019).
[41] McQuade, M "The Untold Story of NotPeyta, The Most Devestating Cyberattack in History", Wired, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[42] Mathews, Lee "NotPeyta Ransomware Attack Cost shipping Giant Maersk Over $200 Million", Forbes, 2017, https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#1206c6df4f9a

[43] Helsel, P & Blackman J "Delta computer outage results in naionwide ground stop". 2018, https://www.nbcnews.com/storyline/airplane-mode/delta-computer-outage-results-nationwide-ground-stop-n913151

[44] Chappell, Bill "Computer Problems Blamed for Flight Delays that Hit U.S. Airlines",2019, NPR, https://www.npr.org/2019/04/01/708738804/u-s-flight-delays-hit-several-airlines-computer-problems-blamed

[45] "National Critical Fuction Set", CISA, https://www.cisa.gov/national-critical-functions-set

[46] Ibid

[47] "Air Carrier Statistics- US Carriers", Department of Transportation, https://www.transtats.bts.gov/Tables.asp?DB_ID=110&DB_Name=Air%20Carrier%20Statistics%20%28Form%2041%20Traffic%29-%20%20U.S.%20Carriers&DB_Short_Name=Air%20Carriers

[48] "Malicious cyber attack leaves airline to cancel flights in Alaska amid peak holiday travel", Associated Press, 2019, https://www.usatoday.com/story/travel/news/2019/12/22/alaska-airline-cancels-flights-after-malicious-cyber-attack/2727709001/

[49] Choi, Gallagher, Harry "An Effect-Centric Approach to Assessing the Risks of Cyber Attacks Against the Digital Instrumentation and Control Systems at Nuclear Power Plants", CISSM, 2020, https://cissm.umd.edu/sites/default/files/2020-02/Risks%20of%20Cyber%20Attacks_DICS%20at%20NPPs.pdf

[49] Harry, C & Gallagher, N "An Effects-Centric Approach to Assessing Cybersecurity Risk", CISSM, 2019,https://cissm.umd.edu/sites/default/files/201907/cissm_risk_framework_overview_final_030119v2.pdf