Navigating Socio-Technical Influences Upon Cyber Resilience Adoption

Travis D. Howard and José de Arimatéia da Cruz

Abstract

Cyber resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, or compromises on systems that use or are enabled by cyber resources. This operational definition adopted from the National Institute for Standards and Technology in Special Publication 800-160 Volume 2, goes beyond technical implementation to include how an organization responds and recovers to adverse effects on information systems; within that response is the ability to continue or fail-over critical system functions even while the system itself is under duress. This chapter presents recommendations for overcoming and adapting to leadership and socio-technical challenges in adopting cyber resiliency. The authors use the 2021 Colonial Pipeline cyber incident to illustrate socio-technical influence factors and make several deductive observations of publicly available information following the incident. The authors make several recommendations for practitioners based on the deductive conclusions drawn from the incident and a 2023 study exploring limiting and enabling factors toward cyber resiliency adoption in organizations based on the Diffusion of Innovations Theory.

Contributors

Travis D. Howard
United States Navy (Retired), Washington, D.C., USA
travis.duane.howard@gmail.com

Jose de Arimateia da Cruz
Georgia Southern University, Savannah, GA & U.S. Army War College, Carlisle, PA
jose.a.dacruz.civ@army.mil

Keywords: Cyber Resilience, Resiliency, Colonial Pipeline, Diffusion of Innovations Theory, Socio-Technical Cybersecurity, Cyber Leadership, Influence Factors

1 Introduction: A Call for National Cyber Resilience

Cyberspace has become a battleground for nation-states and state-sanctioned aggressors. Intelligence testimony to the U.S. Congress in recent years continues to report on a rise in cyber-enabled espionage, intrusion, information theft, and even seeding malware into cyber-physical, industrial control, and critical infrastructure systems that the nation's citizenry depends on (Office of the Director of National Intelligence, 2023).[1] Seemingly in step with the increase in the cyber threat landscape, strategic direction at the U.S. federal level has pivoted decisively toward cyber resiliency as a means to reduce the impact of an attack on critical infrastructure and impose a cost on adversaries attempting it (Office of the President of the United States, 2023).[2]

The authors predict that this call for cyber resilience at a national level will continue and become the dominant strategy for dealing with nation-state threats. This strategic shift represents not a "shield" against attacks, stopping them outright, but rather a "parry and riposte" in which the defender deflects the part of the attack intending to do damage, leaving critical systems intact and leaving open the option for an effective counterattack. In naval combat parlance, legendary strategist and fleet tactics author Captain Wayne P. Hughes, U.S. Navy (retired), advocated for victory through "fire effectively first" (Vencill, 2019).[3] In this case, it would appear that the national cyber strategy to harness resiliency while simultaneously wielding the combat power of the Department of Defense's U.S. Cyber Command would make Captain Hughes proud.

Systems can be engineered and configured for redundancy and rapid fail-over, with segmentation and all the trimmings of engineered resiliency. Yet, organizations and people must adopt resiliency differently through adaptation and leadership. Only when technical and social factors are combined and harmonized can organizations achieve the cyber resiliency needed to sustain operations in this ever-changing digital battleground upon which every internet-connected public and private sector organization stands.

This chapter presents recommendations for overcoming and adapting to leadership and socio-technical challenges in adopting cyber resiliency as an organizational innovation through a case study in recent history that highlights the socio-technical nature of adverse cyber events: the 2021 Colonial Pipeline ransomware event. The authors then present a 2023 study exploring

---

[1] Office of the Director of National Intelligence. Feb 6, 2023. "Annual Threat Assessment of the U.S. Intelligence Community." https://www.intelligence.gov/annual-threat-assessment

[2] Office of the President of the United States. Mar 1, 2023. "National Cybersecurity Strategy." https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[3] Taylor Vencill. 2019. "In Memoriam: Legendary Strategist and Fleet Tactics Author Wayne P. Hughes." Naval Postgraduate School. https://nps.edu/-/in-memorium-legendary-strategist-and-fleet-tactics-author-wayne-p-hughes

limiting and enabling factors toward cyber resiliency adoption in organizations based on the Diffusion of Innovations Theory. The chapter concludes with recommendations for practitioners based on deductive lessons from the 2021 Colonial Pipeline cyber incident and findings from research.

2 Review of the Colonial Pipeline Cyber Event: A Case Study in Socio-technical Cyber Resiliency

On May 7th, 2021, the American public learned that the Colonial Pipeline - responsible for 45 percent of the fuel supply for the East Coast of the United States, had shut down due to a cyber-attack (Marinos & Gordon, 2021).[4] Ransomware inserted by a cyber-crime group known as DarkSide disrupted the company's business network; the operational technology (OT) that ran the 5,500-mile-long pipeline was unaffected. The disruption lasted for six days, and on May 13th, the pipeline resumed delivery to all affected markets, yet the damage was already apparent. The public panic created by fears of fuel shortages caused a supply rush, creating a market frenzy and proof that disruptions to critical infrastructure would yield these results in the future (Marinos & Gordon, 2021).

Two years later, the CEO of Southern Company (a major pipeline operator in the United States, but not the owner of Colonial Pipeline) and the director of the Cybersecurity and Infrastructure Security Agency (CISA) - an agency within the U.S. Department of Homeland Security - issued a joint publication on the progress made as well as a call to action on the work still before them. The CISA release by then-CISA Director Jen Easterly and Sothern Company CEO Tim Fanning (2023) described working groups and public-private partnership efforts that stood up after the incident, including the Joint Cyber Defense Collaborative (JCDC).[5] These groups and initiatives were created to "share insights and information in real-time to understand threats and drive down risk to the nation" (para 2). However, the most impactful statement regarding resiliency came at the end of the release: "We cannot completely prevent attacks from happening, but we can minimize their impact by building resilience into our infrastructure and our society."

---

[4] Nick Marinos and Leslie V. Gordon. 2021. "Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness (infographic)." U.S. Government Accountability Office, WatchBlog. https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic.

[5] Jen Easterly and Tom Fanning. 2023. "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years." Cybersecurity & Infrastructure Security Agency, Blog. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

Scholarly studies to date suggest such resilience continues to elude us. A 2023 study by Greubel, Andres, and Hennecke found articles and media surrounding the Colonial Pipeline incident lacking details and preventative advice that would help students, experts, and the general public understand the need for such resilience, let alone how to achieve it at a technical level.[6] Lubin (2023) analyzed legislative action following the incident and noted a need for more legislative response in the form of reform, regulation, or omnibus legislation that would improve critical infrastructure cyber resiliency.[7] Indeed, Lubin (2023) offered this stark analysis: "The kneejerk litigatory, regulator, and legislative response that the Colonial Pipeline ransomware generated were casebook examples of all wrong with our existing cybersecurity law and policy ecosystem."

The lack of technical details and post-mortem analysis, due in no small part to the pipeline's private-sector ownership, prevents cybersecurity professionals from using the attack as a case for improving resiliency within their corporate networks. Two years after the Colonial Pipeline attack, no correct publicly available data has been collected or disseminated to show that, as a society and a community of cybersecurity experts, we have made progress in building cyber resiliency into critical infrastructure beyond creating collaborative groups to talk about it. In short, lessons learned from the Colonial Pipeline incident are closed and held only for select groups within the public and private sectors. Has Colonial Pipeline improved its socio-technical cyber resiliency? We will have to take their word for it.

3 Understanding Socio-technical Influence Factors in Cyber Resiliency Adoption

Howard (2023), studying on influence factors affecting cyber resiliency adoption, presented nine influences identified and categorized through an extensive literature review.[8] The nine identified influence categories are described in Table 1. The researcher posited that these categories represent socio-technical influences organizations face within the innovation-decision process described within the Diffusion of Innovation (DOI) Theory (Rodgers, 2003).[9]

Influence Factor	Examples

[6] André Greubel, Daniela Andres, and Martin Hennecke. 2023. "Analyzing Reporting on Ransomware Incidents: A Case Study." Social Sciences (2076-0760) 12 (5): 265. doi:10.3390/socsci12050265.
[7] Asaf Lubin. 2023. "Cyber Plungers: Colonial Pipeline and the Case for an Omnibus Cybersecurity Legislation." Georgia Law Review 57 (4): 1605–32. https://search-ebscohost-com.captechu.idm.oclc.org/login.aspx?direct=true&db=aph&AN=169978264&site=eds-live.
[8] Travis D. Howard. 2023. "Understanding Influence Factors in Cyber Resiliency Adoption: A Mixed Methods Study of Cybersecurity Leaders." PhD diss. Capitol Technology University.
[9] Emmett M. Rodgers. 2003. "Diffusion of Innovations" (5th Ed.). Free Press.

Technical	Network topology, implementation frameworks, system engineering and design concepts, system security architecture
Cultural	Workplace culture and norms, cybersecurity awareness and agency, cultural adaptability to change, innovativeness characteristics
Organizational policies and leadership	Governance models, leadership and executive level support, policies, procedures, standards, guidelines
Workforce and skills	Qualifications, engagement skills and subject matter expertise, roles and responsibilities, team structures
Knowledge management and information access	Access to information, ability to categorize, organize, and share knowledge
Industry and competitiveness	Competitive advantage, industry infrastructure and characteristics, business-to-business factors, business-to-consumer factors, public or private ownership
Vendor and third-party support	Managed cloud providers, external consultancies, staffing agencies, software and hardware vendors, patching and update support for installed products
Legal and regulatory	Privacy and civil liberty issues, industry specific laws and regulations, organizational legal concerns to prevent lawsuits
Resources	Access to: financial resources, human resources, technological and material resources, rapid access to tap resources for innovations, ability to sustain funded efforts

Table 1: Socio-Technical Influence Factors Affecting Cyber Resiliency Adoption

Emmett Rodgers, first in 1962 then refined through several revisions until 2003, developed the DOI Theory to explain how innovation spreads through a social system. It is best known for the "bell curve" model, which describes the momentum of innovation through consumer groups

known as innovators, early adopters, early majority, late majority, and laggards. Perhaps lesser known, Rodgers (2003) also postulated vital elements and characteristics of an innovative organization and the process by which organizations decide whether to adopt or reject an innovation, known as the innovation-decision process model (IDPM).

The IDPM is a five-step decision-making process (Figure 1). Ryan and Gross identified the concept in 1943 in their diffusion study. Rodgers's seminal work, *Diffusion of Innovations 5th edition* codified the concept into the literature. Before the first step, conditions influence the process, such as a felt need or problem to be solved, the organization's overall innovation characteristics, and the social system's norms. Then, the knowledge phase occurs when the organization gathers awareness and information about the innovation, informed and influenced by the prior conditions. The organization is then persuaded to analyze how the innovation would benefit the whole (persuasion phase). Once the decision has been made, it is either adopted or rejected by the innovation (decision phase). In the implementation phase, if adopted, the innovation is implemented, and a confirmation phase determines over time if the decision made was correct for the organization (Rodgers, 2003).

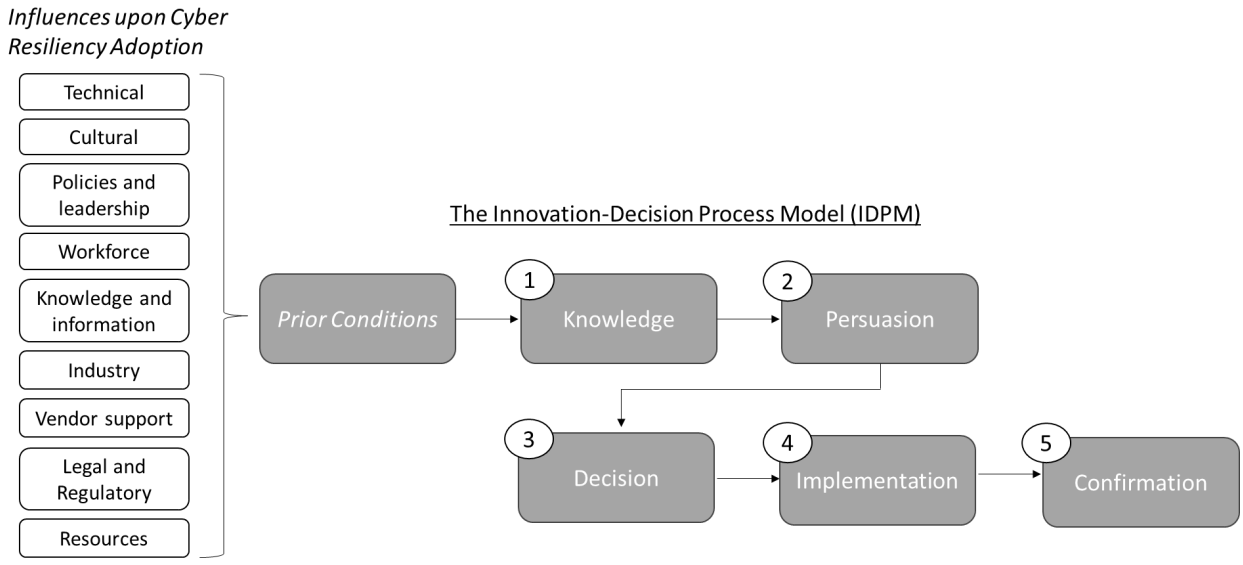

Figure 1: The nine cyber resiliency influence categories feed the *prior conditions* pre-requisite to the IDPM (Left) and Socio-Technical Influences upon the IDPM for Cyber Resiliency Adoption (Center).

The 2023 study found that technical factors - such as implementation frameworks, network topologies, software and hardware designs, and available architecture - enabled overall (85.51%) versus limited (78.26%) adoption. Organizational influences such as internal policies, procedures, and leadership were high in percentile and found near-equally enabling (84.05%) as limiting

(85.51%). Resources and funding were, predictably, overall limiting (85.95%) vice enabling (73.91%). These findings show that technical advances enable cyber resiliency adoption in organizations, while a lack of resources limits adoption and sustainment. Internal policies and leadership were significant influences and could limit or enable cyber resiliency adoption depending on the organization's characteristics (Howard, 2023).

Participants in the 2023 study noted significant influences around workplace culture, organizational policies, practices, and leadership buy-in that led to either limiting or enabling factors towards cyber resiliency adoption or sustainment of the adopted capability as a part of cyber defense. Organizational cyber leaders, such as the Chief Information Security Officer or senior-level managers and directors of cybersecurity programs, noted that strong leadership on their part coupled with executive-level championship was essential to success. Cultural barriers around resistance to change were experienced, and some participants experienced headwinds in the form of internal politics and a lack of clear prioritization that led to funding shortfalls (Howard, 2023).

4 Deconstructing the Influence Factors in the Colonial Pipeline Cyber Incident

While little actual data is publicly available to researchers in analyzing lessons learned from the 2021 Colonial Pipeline cyber incident, deductive reasoning combined with what information is available could allow practitioners and researchers alike to understand the possible socio-technical influence factors affecting cyber resiliency adoption in this case. One must first examine what is known, thanks to an excellent summation of events by the previously referenced Asaf Lubin (2023) in the *Georgia Law Review*:

1. The DarkSide ransomware attack affected the Colonial Pipeline business network and did not affect the pipeline's industrial control systems (ICS) (pp. 1609-1610).
2. The pipeline ceased operations due to an inability to perform business functions such as delivery tracking and billing (pp. 1609-1610).
3. The pipeline's owners paid a ransom of $4.5 million (USD) worth of Bitcoin in exchange for decryption keys to restore their business network (p. 1611).
4. Following the incident, the U.S. Government recovered all the ransom and almost eliminated the DarkSide ransomware gang (pp. 1612-1613).

Unfortunately, at the time of writing, no technical information exists in the form of Colonial Pipeline's business network topology (before and after the incident took place), nor can

anyone outside of the organization genuinely understand internal policies and leadership factors, which were identified as significantly influential in the 2023 study on cyber resiliency influence factors. Further, no programmatic overviews, policy statements, or press releases related to cybersecurity can be found on Colonial Pipeline's public website, despite a "Safe Operations" section that highlights environmental safety and emergency preparedness outside of the cyber domain (such as spills and contamination).

Despite an unfortunate lack of publicly available data, several deductions can be made. Before the incident, many factors that influenced the adoption of cyber resiliency in Colonial Pipeline's business network were low to moderate. Technical aspects such as the suitability of the network topology to resiliency architecture and the general availability of resilient system security engineering would have appeared moderate. Likewise, the availability of knowledge and information on cyber resiliency as an accepted systems engineering practice and implementation frameworks such as the U.S. National Institute for Standards and Technology (NIST) special publication (SP) 800-160 Volume 2 could be considered moderately influential. Finally, vendor support was available through commercial procurement to support cyber resiliency adoption, indicating at least a moderate level of influence favoring adoption. Based on the phenomenological results of the 2023 study on influences upon cyber resilience adoption, one might deduce a low level of influence favoring cyber resiliency adoption within Colonial Pipeline for cultural, organizational, industry, legal, and resource categories – indicating the demand signal for such adoption was not present before the incident; otherwise, at least rudimentary procedures would have been in place to operate the business side of Colonial Pipeline without networked software and hardware to support. Table 2 summarizes levels of influence favoring cyber resiliency adoption before the 2021 ransomware incident.

Influence Category	**Possible Level of Influence Favoring Adoption**
Technical	Moderate
Cultural	Low
Org Policies and Leadership	Low
Workforce	Low
Knowledge and Information (availability)	Moderate
Industry	Low
Vendor Support	Moderate
Legal and Regulatory	Low

Resources and Funding	Low

Table 2: Socio-technical factors affecting cyber resiliency adoption on Colonial Pipeline *before* the 2021 ransomware incident.

Post-incident, social pressures were exerted on Colonial Pipeline and the U.S. Government to prevent such an incident. The 2021 ransomware incident sparked several journal, scholarly, and media articles on the subject, and the U.S. Government formed several working groups and public-private collaboration initiatives as a result (Easterly & Fanning, 2023). Technical, knowledge and information, and vendor support remained moderately influential as little had changed. Yet the social factors likely increased, particularly organizational policies and leadership (indicating a desire to change policies and procedures to prevent a recurrence), industry (pressure from other pipeline operators to understand what happened to mitigate their vulnerabilities), and regulatory influence in the form of a significant amount of government "attention" (despite any actionable legislation that resulted from it). Resources were made available to mitigate vulnerabilities to the business network and implement changes to the company's overall emergency preparedness for cybersecurity. Table 3 summarizes where influence factors changed post-incident.

Influence Category	**Possible Level of Influence Favoring Adoption**
Technical	Moderate
Cultural	**Moderate**
Org Policies and Leadership	**Moderate to High**
Workforce	Low
Knowledge and Information (availability)	Moderate
Industry	**Moderate**
Vendor Support	Moderate
Legal and Regulatory	**Moderate to High**
Resources and Funding	**Moderate**

Table 3: Socio-technical factors affecting cyber resiliency adoption on Colonial Pipeline *after* the 2021 ransomware incident.

Did Colonial Pipeline improve its cyber resiliency due to what it may have learned from this incident? Had a manual method to track pipeline deliveries and conduct billing been

implemented, could the pipeline have remained operational through the incident response process? Only Colonial Pipeline can definitively answer such questions; presented in this chapter are the authors' estimations and deductions based on limited publicly available data and by extrapolating results from the 2023 study on influences upon cyber resiliency adoption. Yet this thought experiment yields some interesting observations that many cybersecurity practitioners already know to be true: nothing spurs cybersecurity actions better than a significant cyber incident. One can see how the IDPM for Colonial Pipeline could have been influenced when mapped to socio-technical influence categories. The challenge to practitioners, therefore, must be to affect these influence factors in favor of resiliency adoption before such an incident occurs.

5 Recommendations for Practitioners

Deductive analysis of the 2021 Colonial Pipeline ransomware incident using the socio-technical influences upon the innovation-decision process model allows the authors to present recommendations along the probable five influence factors that may have increased the likelihood of resiliency adoption for Colonial Pipeline post-incident: cultural, organizational, industry vertical, legal, and regulatory, and resources.

Cultural: Respondents in the 2023 study on influences upon cyber resiliency adoption indicated that cultural resistance to change was among the most limiting factors (Howard, 2023). Adopting resiliency practices that change how the workforce operates—such as training on manual processes or running drills that involve suspending automation to test the effectiveness of resiliency protocols—will be a tough sell to a resistant workforce. Overcoming this influence factor as a limiter can be twofold. First, concentrate on automated resiliency methods, such as automated fail-over and network segmentation with single sign-on (SSO) capabilities, that make it easy for the workforce to adopt or bypass cultural adoption altogether. Secondly, when techniques and procedures must be changed to incorporate resiliency, do so over a more extended period, emphasizing over-communication to allow the workforce time to absorb information and adapt to change.

Organizational policies and leadership: While understanding the technical aspects of their cyber defense programs is essential to the job, organizational cyber leaders must now shift to understanding the business at a deeper level to align with priorities and "tell the story" to executive leadership and the board of directors. Doing so generates executive buy-in essential for implementing new capabilities affecting the entire organization, such as cyber resiliency adoption. Leaders must communicate resiliency as a "whole of company" solution to vulnerabilities that, if or when exploited, would cause significant damage - not just a purely technical solution that can be implemented "behind the scenes." Respondents in the 2023 study on influences upon cyber

resiliency adoption noted that executive championship was essential to successfully adopting cyber resilient capabilities (Howard, 2023). Cyber leaders should identify and ally with other influential executives who can sway decision-making or help communicate the necessity of resiliency measures, such as the Chief Risk Officer or Chief Operating Officer. Daily revenue loss due to a cyber incident can be calculated, which can bring the Chief Financial Officer around to support these capabilities as well.

Industry: Influences from the industry vertical or market segment can be complex to understand, let alone be predicted. Business strategies are crafted to compete within the market segment the organization finds itself within, or in the case of the public sector, better serve the population. As a cyber leader struggles to understand influence factors affecting the industry, they find that scholarship and networking are required. For the former, adopting an always-learning mindset enables leaders to challenge their thinking in favor of what innovations are possible in the market segment - not just technical but social to include different ways to examine problems or perform tasks. For the latter, many industries host conferences, summits, and working groups that include cybersecurity as a topic, and leaders should participate directly or send representation. Furthermore, cyber leader must also implement resilience-by-design approaches that "enhance the ability of critical infrastructure to prepare for, adapt to, and recover from changing conditions presented by new and emerging threats and hazards" (The White House, 2024, p. 22).[10] This ensures that industry-affecting innovations are known and issues affecting the industry can be understood and acted upon before they become legal or regulatory headaches.

Legal and regulatory: Speaking of headaches, nothing brings one on faster than a new law or regulatory requirement that forces change upon an organization. While "compliance" is often regarded as a "dirty word," cyber leaders have learned to embrace it to generate the adoption of cybersecurity and cyber resiliency capabilities. As such, cyber leaders are advised to take full advantage of changes to laws and regulations that involve cyber resiliency to increase their adoption rate and generate resources in favor of implementing higher levels of resiliency. However, leaders are cautioned not to over-rely on such methods lest they backfire when laws change, or regulations are rolled back depending on the socio-political landscape.

Resources: Consider again the case of the 2021 Colonial Pipeline cyber incident: while much government attention was received, it did not result in regulatory action or legislation (Lubin, 2023). Suppose a leader were to rely on the threat of legal or regulatory action alone; in that case, they might experience a "rubber band" effect where early support for adoption is achievable only to wane in the "confirmation" phase of the IDPM. A measured approach is therefore recommended, balancing the call to action (and funding) that laws and regulations create with

[10] The White House. April 30, 2024. "National Security Memorandum on Critical Infrastructure Security and Resilience," available at National Security Memorandum on Critical Infrastructure Security and Resilience | The White House. Accessed May 2, 2024.

sustainable and affordable resiliency capabilities that can endure long after the initial surge of support has passed.

6 Conclusion

True organizational cyber resiliency considers not just technical but social factors, especially considering that fact the "in the 21st century, the United States will rely on new sources of energy, modes of transportation, and an increasingly interconnected and interdependent economy" (The White House, 2024, p. 2). Socio-technical influences upon cyber resiliency adoption must be understood if such resiliency is to be achieved, particularly in critical infrastructure, as called for in national strategy and policy circles. This is not just a government problem to solve; every organization is affected by adverse cyber events, and when critical infrastructure is threatened, it affects society as a whole and - depending on severity - has repercussions in the global economy. It is up to cybersecurity leaders in every organization to take charge and ensure their organization can withstand, adapt to, and recover from adverse cyber events.

What ties these influence factors together is strong leadership on the part of the senior-most cybersecurity executive (Chief Information Security Officer-CISO) that communicates a clear vision and roadmap for adoption, provides direction to both internal staff and external stakeholders, but perhaps most importantly, inspires others to see what they see: an organization capable of not only defending against attacks but continuing essential functions despite them; to do so stop cyber attackers before they carry out their nefarious activities and achieve their ultimate goal.

Bibliography

Easterly, Jen and Fanning, Tom. "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years." Cybersecurity & Infrastructure Security Agency, Blog. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years. 2023.

Greubel, André, Andres, Daniela, and Hennecke, Martin. "Analyzing Reporting on Ransomware Incidents: A Case Study." Social Sciences (2076-0760) 12 (5): 265. 2023. doi:10.3390/socsci12050265.

Howard, Travis D. "Understanding Influence Factors in Cyber Resiliency Adoption: A Mixed Methods Study of Cybersecurity Leaders." Ph.D. diss. Capitol Technology University. 2023.

Lubin, Asaf. "Cyber Plungers: Colonial Pipeline and the Case for an Omnibus Cybersecurity Legislation." Georgia Law Review 57 (4): 1605–32. 2023. https://search-ebscohost-com.captechu.idm.oclc.org/login.aspx?direct=true&db=aph&AN=169978264&site=eds-live.

Marinos, Nick and Gordon, Leslie V. "Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness (Infographic)." U.S. Government Accountability Office, WatchBlog. 2021. https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic.

NIST Special Publication 800-160, Volume 2, Revision 1. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. Available at https://safe.menlosecurity.com/https://doi.org/10.6028/NIST.SP.800-160v2r1. Accessed May 2, 2024

Office of the Director of National Intelligence. "Annual Threat Assessment of the U.S. Intelligence Community." Feb 6, 2023. https://www.intelligence.gov/annual-threat-assessment.

Office of the President of the United States. "National Cybersecurity Strategy." Mar 1, 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

Rodgers, Emmett M. *Diffusion of Innovations* (5th Ed.). New York: Free Press. 2003.

The White House. April 30, 2024. "National Security Memorandum on Critical Infrastructure Security and Resilience," available at National Security Memorandum on Critical Infrastructure Security and Resilience | The White House. Accessed May 2, 2024.

Vencill, Taylor. “In Memoriam: Legendary Strategist and Fleet Tactics Author Wayne P. Hughes.” Naval Postgraduate School. Dec 11, 2019. https://nps.edu/-/in-memorium-legendary-strategist-and-fleet-tactics-author-wayne-p-hughes.