Reimagining Resilience:

Managing Critical Infrastructure Risks in the Digital Age

By: Suraj Raghupathy

The cornerstone of a functioning society and economy is its critical infrastructure systems which include physical, virtual and human components. Critical infrastructure systems are vital to everyday life due to their complex interdependencies and the severe risks to public health, safety and security if compromised. The U.S. department of homeland security has identified four sectors[1] of critical infrastructure – Water and Wastewater Systems, Energy, Transportation Systems, and Communications as lifelines for the community since they enable the operations of all other sectors.

Consumerization of IT and the rise of advanced technologies such as Cloud Computing, Virtualization, Edge Computing, 5G, Private Long-Term Evolution (LTE), Blockchain, Robotics, Augmented Reality, Digital Twins, Internet of Things (IoT), Artificial Intelligence (AI) are driving efficiency and transforming critical infrastructure sectors. This is illustrated in **Figure 1**.

FIGURE 1
DIGITAL TECHNOLOGY USE IN CRITICAL INFRASTRUCTURE SECTORS

Critical Infrastructure Sector	Critical Infrastructure Sector	Physical Components	Virtual Components	Sector-Specific Use Case
Communications	5G, Private LTE, Edge computing, Virtualization	Base stations, satellites, and fiber optic cables, cell towers	Network slice, cloud orchestration platforms, software defined network components like firewalls, load balancers, etc.	A dedicated 5G network slice allocated to first responders for uninterrupted communication during a natural disaster, powered by AI tools at the edge to route traffic.
Energy	IoT, Cloud Computing, AI, Smart Grids	Transformers, substations, transmission lines, smart meters with sensors	SCADA system for monitoring, AI powered smart grid platforms for load balancing	A regional utility company uses smart meters with sensors to transmit real-time consumption data to AI models to optimize energy distribution dynamically.
Transportation Systems	IoT, AI, Cloud Computing	Airports, railway networks, seaports, roads, bridges, and traffic control systems	AI based logistics tool, cloud-based fleet management systems, autonomous vehicle control systems, sensor equipped traffic monitoring networks	Subway transit system uses AI powered routing systems and IoT track sensors to monitor train conditions in real time and reduce service disruptions.
Water and Wastewater Systems	IoT, AI, Cloud Computing	Pipes, pumps, valves, chemical dosing systems, water quality sensors, treatment plant machinery	SCADA systems, IoT sensor networks, AI driven analytics for leak detection and system optimization	Municipal water departments gather data from integrated IoT sensors on physical components to feed AI analytics within SCADA platforms to monitor flow and detect leaks in real time.

According to a 2024 Verizon Mobile Security Index Report[2], nearly 95% of all critical infrastructure organizations now use IoT devices, particularly for physical security (61%), monitoring system efficiency (52%), and delivering digital services (52%). Many of the critical infrastructure sectors have made great strides in digital growth, however this is directly linked to emerging risk profiles.

Understanding the threat landscape in critical infrastructure sectors

Digital technologies have led to complacency in how we rely on critical infrastructure systems. The inability of cyber security safeguards to keep pace with a rapidly shifting threat landscape has led to advanced threats and vulnerabilities, undermining the perceived benefits of these technologies for critical infrastructure. The convergence of connected IT infrastructure and these emerging technologies expands the attack surface significantly (and uniquely so). Here are some ways the use of IoT, AI, Cloud computing and 5G in critical infrastructure increases exposure:

- **IoT** - It might seem apparent that industrial IoT has revolutionized real-time monitoring and control across sectors such as structural integrity in bridges, pipeline pressure in energy systems, water treatment quality and manufacturing systems. However, this has also precipitated supply chain risks as components that were never designed with security in mind are internet exposed. When operated outside traditional security perimeters, they lack baseline controls – such as strong passwords for legacy systems, multi-factor authentication, secure encrypted communication, timely patching firmware, etc. This enables botnet attacks (e.g., Mirai), unauthorized remote control, lateral movement for deeper system compromise, and data exfiltration. The risk impact upon exploitation includes loss of confidentiality through leaked operational data, integrity via sensor spoofing, availability of service through Distributed Denial of Service (DDoS) attacks using ephemeral botnets.
- **Cloud Computing** - Virtualization technologies and cloud-based environments have enabled rapid elasticity and central management of data and applications – transforming sectors like healthcare through electronic patient records, energy with remote utility billing platforms and smart grid analytics, and transportation via real time fleet coordination and signaling systems. Although cloud environments support customization, scalability and disaster recovery capabilities, it is not without significant security tradeoffs. Configuration management is still an administrative overhead for users and relying on third party cloud service providers does not eliminate the risk from misconfigured virtual machines (VMs), exposed application programming interfaces (APIs), overly permissive identity and access management (IAM) roles and inadequate key management. These vulnerabilities open the door to credential theft and lateral movement, privilege escalation, data breaches from exposed cloud resources, and ransomware attacks targeting cloud storage. Exploitation of these vulnerabilities can lead to the compromise of sensitive operational and personal data (confidentiality), manipulation of control signals or records (integrity), and interruption of essential services or applications. So, the risks posed to public safety and infrastructure resilience can be telling. In 2017, an improperly configured cloud storage bucket[3] inadvertently exposed the personal information of close to 50,000 employees from government agencies, banks, and a utility company in Australia. Since cloud environments in the context of critical infrastructure means storing large volumes of highly sensitive information, they are lucrative targets for ransomware attacks.
- **Artificial Intelligence** - AI based automation when integrated with operational technology supports autonomous decision-making and efficient predictive maintenance. The AI's foray into critical infrastructure is undeniable – It is used for demand forecasting and power distribution in the energy sector, diagnostic imaging and patient triage in healthcare, quality control and defect identification in the manufacturing sector. This widespread adoption makes critical infrastructure targets for data driven attacks. AI models come with a data dependence, making them susceptible to manipulation and false negatives when fed with carefully crafted data. In a high stakes environment like critical infrastructure this often means outages or physical damages. Traditional security tools fail to detect malicious data poisoning, model tampering or abuse via exposed machine learning APIs, and manipulation of control logic through adversarial input. AI doesn't always get it right and here's why that's risky. With the lack of adequate input validation, risk of unverified training data being used in continuous learning setups, absence of fail-safe mechanisms (in case of invalid AI decisions), and model drift over time, there are multiple pathways for exploits. These weaknesses can lead to integrity breaches through incorrect or manipulated predictions, confidentiality loss from exposure of sensitive training data, and service disruptions if AI systems are disabled. In the worst-case scenario, autonomous systems can instantaneously launch attacks at scale upon compromise causing widespread harm to human safety – and making containment and manual override very difficult.
- **5G and Private LTE** - Advanced wireless communication technologies complement wired or wi-fi based connectivity and provide fast, reliable connections that suit device-dense environments. When you look at critical infrastructure, mobile command centers, public safety LTE for police, fire, or emergency medical services, connected traffic management systems, field operators in manufacturing, and remote surgery networks often leverage 5G and private LTE where real time responsiveness is an absolute necessity. However, adoption of 5G is accompanied by cyber risks that come from bad network configurations, insecure virtual tools (think firewalls, routers, switches and gateways), weak isolation in virtual systems, and vulnerabilities in edge devices. Cross-domain compromise can stem from the exploitation of protocol-level vulnerabilities (e.g., lack of session validation, unfiltered packets, session hijacking), misconfigurations in network slicing allowing unauthorized sniffing or lateral movement, and the manipulation of edge nodes within industrial systems through malicious code injections. The resulting impact includes loss of service, integrity of operational commands, and unauthorized control over safety critical systems. What really turns the dial up is the amplification of these effects due to the distributed architecture of networks in critical infrastructure environments.

The True Cost of Disruption in Critical Infrastructure

Sophisticated digital exploits and malicious actors are targeting essential services, government facilities and public infrastructure that have no tolerance for downtime more than ever before - posing serious consequences that can disrupt societies. Here are four consequences that underscore the gravity of cyber threats to critical infrastructure.

- **Human Safety** - Cyber-attacks on systems like hospitals, water treatment facilities, or transportation networks are not just about data or downtime; they can cause real-world physical harm or fatalities, directly endangering human lives.

In February 2024, Change Healthcare, a subsidiary of the UnitedHealth Group was struck by a ransomware attack (ALPHV/BlackCat) carried out by foreign adversaries. A significant amount of data was encrypted, including personal information, payment details, insurance records, and other sensitive information – and the threat actors demanded a ransom of $22 million for its recovery.[4] The incident affected the delivery of healthcare services by delaying access to critical medical information, endangering the safety of patients. It also threatened the solvency of healthcare providers dependent on Change Healthcare, forcing some to take out private loans or pull from cash reserves. Similarly, cyber-attacks on transportation infrastructure like air traffic control networks and rail signal systems could result in fatal crashes or derailments if systems are adversely manipulated or taken offline even for a short duration.

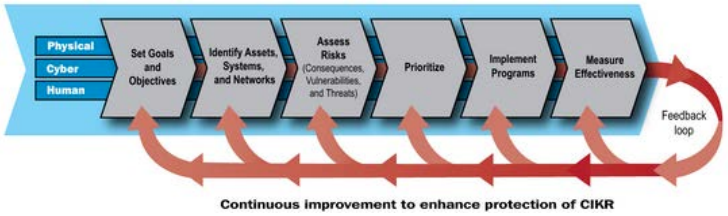
- **Cross Sector Cascading** - The interdependent and fragile nature of the critical infrastructure sectors means an attack inflicted on one sector likely cascades to other sectors or even countries leading to large-scale damage that can debilitate communities. These interdependencies are often underestimated in critical infrastructure risk planning. For example, the Canadian and U.S. energy grids are closely interconnected[5], and so a cyber-attack affecting power supply in the U.S. can cripple essential services in Canada such as hospitals, telecommunications, transportation systems, and water treatment plants – all of which depend on stable power to function. Such disruptions can snowball and easily overwhelm response capabilities well beyond the initial target.
- **National Security and Geopolitical Implications** - Critical infrastructure attacks can severely impair national sovereignty, global standing and defensive readiness. In 2016, a Russian hacking group named Sandworm launched a multi-vector attack on a Ukrainian power facility. The attack comprised of a malware deployment (BlackEnergy3) with a destructive KillDisk program[6] that wiped hard drives, in conjunction with spear phishing, stolen credentials, VPN access, remote exploitation tools to compromise systems. Approximately 700,000 people in Ukraine lost power in the middle of December as a result – illustrating how state-sponsored cyber-attacks can be used to assert regional influence. So, strengthening a nation's commitment to baseline protection and cyber resilience requires much effort, especially in countries with limited state capacity.
- **Long-Term Operational and Recovery Costs** - Recovery from a cyber-attack on critical infrastructure often includes system forensics, software patching, regulatory compliance reviews, and infrastructure overhauls. However, it does not end once systems are back up and running – it can be a lengthy, resource-intensive and expensive process. In 2017, the NotPetya cyberattack[7] took down global shipping company Maersk, halting operations at 17 international ports and disrupting nearly 20% of the world's maritime trade. The malware wiped out 4,000 servers and 45,000 devices, forcing Maersk into a long recovery effort that lasted weeks, and included physically transporting a surviving backup server from Ghana. Maersk's recovery costs were estimated to be close to $300 million, with additional ripple effects across global supply chains. This case highlights how cyber-attacks on critical infrastructure can have lasting operational and financial consequences even for organizations with strong resilience capabilities.

There is no doubt that cyber practitioners must clearly understand which threats truly matter as well as how to address them effectively. To that end, they often lean on established industry frameworks as a starting point, and this is where the challenges and problems begin.

Operationalizing the Framework: The Hard Part

In theory, there are security frameworks that can be adapted towards critical infrastructure risks such as the Zero Trust [8] paradigm for industrial infrastructure and the NIST AI Risk Management framework[9], released in January 2023 to guide organizations in managing socio-technical risks posed by the use of AI. The department of homeland security has developed the National Infrastructure Protection Plan (NIPP) with a coordinated risk management framework to minimize the impact of attacks on critical infrastructure by leveraging federal resources. The components of this framework are depicted in (**figure 2**)[10].

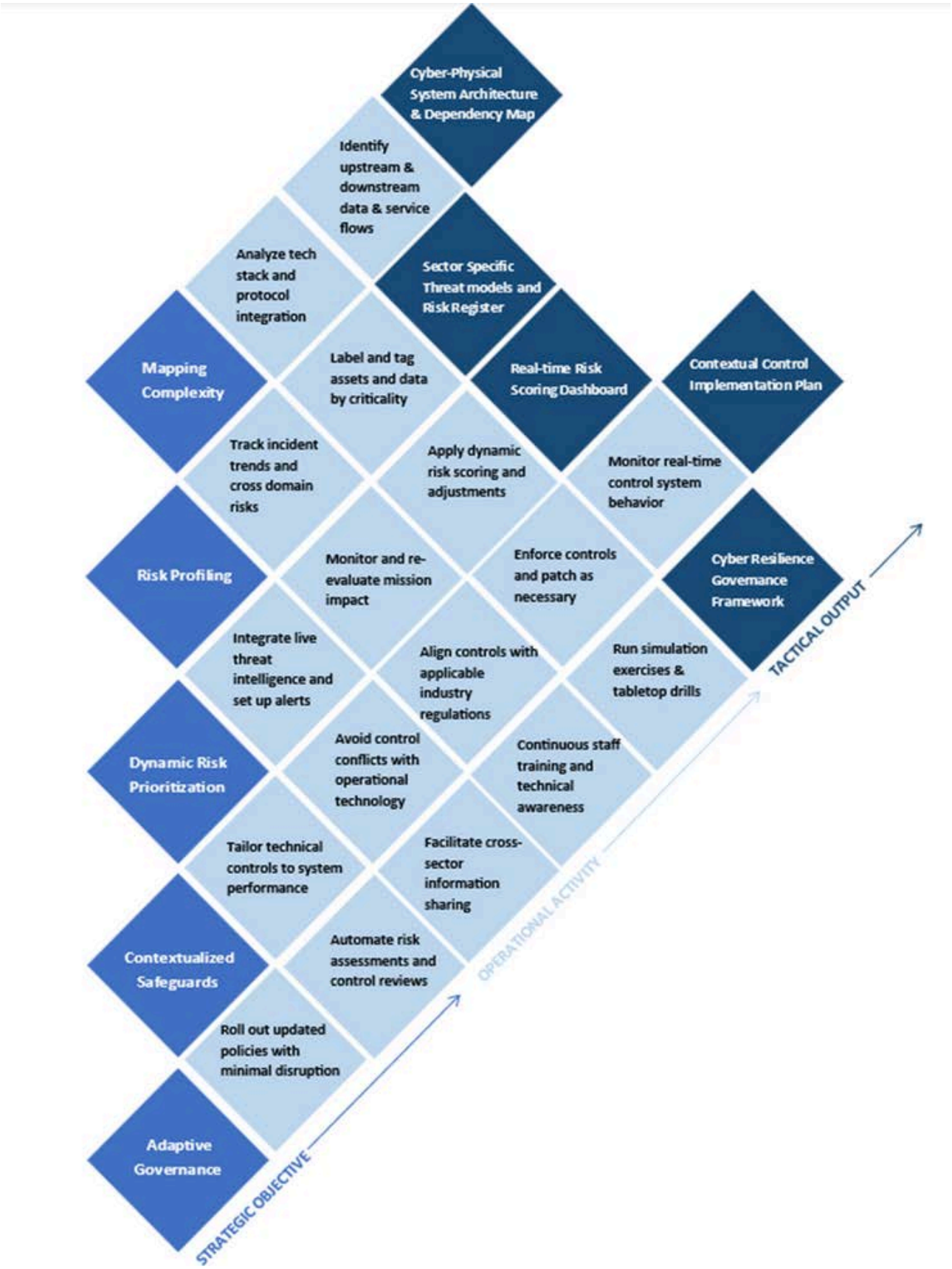
FIGURE 2
NIPP Risk Management Framework



Source: U.S. Department of Homeland Security; "National Infrastructure Protection Plan", https://www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf

There is also the Network and Information Security Directive (NIS2) directive that requires organizations in the EU to both put safeguards in place and demonstrate they work. While interest in these frameworks is growing, many organizations in the critical infrastructure sectors still do not consider these options, missing out on valuable guidance. Also, interest does not always translate into action, and organizations often hit roadblocks when trying to apply these frameworks. This is because in practice, cyber-attacks still happen since any number of things can go wrong when executing these broad, foundational frameworks into sector specific actions – especially within real world resource limitations, operational constraints and industrial contexts. Moreover, it is impossible to overlook the proverbial weakest link in cybersecurity – people. After all, the onus of implementing these frameworks is a shared responsibility for the critical infrastructure community – comprised of public and private owners and operators, and other stakeholders. Tackling these challenges means rethinking how we understand, manage and share risk. To achieve this, a layered approach with strategic, operational, and tactical dimensions (**figure 3**), needs to complement these frameworks. This approach can then be integrated with regulatory compliance requirements, domain expertise, industry best practices and adjusted over time to address sector-specific needs.

FIGURE 3
Cyber Resilience Execution Approach



Key Considerations before implementing Critical Infrastructure Risk Management

The question arises as to how to close the gap between frameworks and effective execution. Adopting a responsive management approach helps in aligning risk efforts with real-world needs and operational realities. Here are 5 considerations to be addressed when mitigating emerging threats in critical infrastructure:

1. Map technological complexities with system dependencies – From an attack surface perspective, grasping how technologies integrate and interact within each sector is paramount. It is not always obvious that physical service interruptions are often caused by upstream and downstream risks in critical infrastructure – many of which originate in IT. For example, smart meters in the energy sector use third party mobile networks and data collectors to send data to utility providers that host backend systems in cloud environments. If the in-scope telecom network goes down or the cloud infrastructure is compromised, power delivery to homes is affected. Assessing how systems, technologies and data operate within each sector's environment can reveal potential attack vectors, single points of failure, data exfiltration risks and cross-domain vulnerabilities. This mapping exercise clarifies how cyber risks become physical risks using IT-OT architecture diagrams, data flow maps, asset inventories, etc. A blueprint for analyzing the attack surface and threat modelling can be created by looking at several factors:

- What is the mission-critical function and what technologies enable them?
- What devices, platforms, network interfaces and protocols are in use to connect legacy operational technology with modern IT systems?
- What types of data are collected and how is data stored, processed, or transmitted?
- What external vendors, cloud services, or third-party APIs are integral to operations?
- Which physical processes rely on digital inputs (e.g., power shutoff, automated braking systems, opening or closing valves)?
- How can one system's failure trigger failures in other systems or sectors?

2. Define contextualized risk profiles – Often in critical infrastructure, sector-wise differences persist not just in operations, technologies used, or data flows – there are differences in cyber threat exposure and potential impact on society.For instance, some sectors are targeted by threat actors more than others. Per Statista[11], citing data from the European Repository of Cyber Incidents (ERCI), out of 450 attacks on the critical infrastructure sectors in 2023, the healthcare sector was the hardest hit, making up 14.2% of critical infrastructure attacks, while financial services were next at 8.3%, followed by telecom, transport, and energy sectors. If impact is considered, the same technical risk can lead to different consequences depending on where and how it strikes. For example, in the financial sector, a ransomware can encrypt core banking systems and disrupt transaction processing and payment platforms, while in healthcare, ransomware attack can target Electronic Health Records (EHRs) and hospital. The same threat (ransomware) that causes financial inconvenience in one sector can cause catastrophic failure in another by affecting patient care and safety. Hence, maintaining granular risk visibility is key. Risk assessments of varying depths must be conducted for each critical infrastructure sector to identify cyber risks specific to the operational and technological environment, and risk appetite.

3. Adapt for point-in-time risk prioritization – The issue with sector-specific risk profiles is treating risks as snapshots in time – while threats evolve rapidly in critical infrastructure. To stay focused on what matters most, a dynamic risk matrix to assess and re-prioritize risks near real time should be incorporated. To take this idea further, live threat intelligence should be integrated into risk models – such as feeds on new ransomware strains, zero-day vulnerabilities, patch status, known exploits, etc. Tapping into sector-specific advisories must be encouraged including from Information Sharing and Analysis Centers (ISACs), and alerts from United States Computer Emergency Readiness Team (US-CERT) and Cybersecurity & Infrastructure Security Agency (CISA). This allows risk scores to be dynamically adjusted (usually elevated) as the threat changes, even if the baseline risk for the threat was previously considered low. Secondly, when calculating risk impact, it is important to move away from viewing an attack only as a technical compromise or failure. The more important aspects are – maintaining safety and determining how essential each system or asset is to delivering critical services. So, the actual impact is not just about what fails, it is also about when, where, and how long it fails. Lastly, interdependency risks identified should be factored into risk scoring to suitably prioritize risks that can quickly escalate or cascade into other sectors.

4. Deploy safeguards for operational fit – Implementing effective controls in critical infrastructure environments means aligning security measures with the realities of the attack surface without getting in the way of operations. Fit-for-purpose safeguards must be engineered by considering technical architecture and physical constraints of the sector. One piece of the puzzle to ensure resources are not wasted on the wrong controls. For instance, applying encryption to all data in transit could be a best practice, but when applied in an industrial control loop or emergency dispatch networks, it can interfere with system behavior or delay safety-critical responses. Similarly, blanket audit logging across all endpoints does not add value unless those logs are aligned with key operational events such as medication administration in healthcare or control room overrides in a power plant. And the other piece is making sure vulnerabilities that matter the most are not missed, considering not all threats carry the same weight in every sector. A bank might focus on protecting transactions from DDoS attacks, while a power utility may want to isolate SCADA systems from the internet using network segmentation and strict access controls.

5. Establish agile governance models – Both the COBIT 2019 framework[12] and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 published in 2024, recognize governance as a key driver of risk management[13]. In the context of critical infrastructure, resiliency cannot be built in the absence of ongoing monitoring and flexible governance. Similar to continuous threat monitoring, cyclical risk assessments and control effectiveness checks should be performed to stay on top of new system changes and evolving threats. Governance models should support the roll out periodic policy updates without disruption and also facilitate workforce training – both technical role-based training and social engineering awareness. Reinforcement through simulation testing, tabletop exercises, and post-incident lessons learned is critical for validating readiness and continuous improvement. Lastly, sharing threat intelligence with federal, Federal, state, local, tribal, territorial, and private sector partners across sectors is essential for a stronger response to potential attacks. The last thing that organizations and agencies want is a siloed structure that impede communication and alignment between stakeholders. Teamwork and coordination between sectors and partners can localize damage and prevent regional or nationwide impact.

The Path Forward for Managing Critical Infrastructure Risk

The critical infrastructure ecosystem has become more complex and interconnected through digital technologies such as AI, IoT, and Cloud Computing, etc. There is a growing need to move beyond traditional approaches to risk management and start with context. Risks and risk management in critical infrastructure should not be generalized, and it is a necessity to evaluate risk in context with tailored tactics and safeguards proportional to sector-specific vulnerabilities. A continuously evolving risk management approach that adapts to the shifting threat landscape is the key to build resilient critical infrastructure.

References

1. Cybersecurity & Infrastructure Security Agency. (n.d.). Critical infrastructure sectors. U.S. Department of Homeland Security. Retrieved June 10, 2025, from https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
2. Verizon. (2024). 2024 Mobile Security Index. Retrieved June 10, 2025, from https://www.verizon.com/business/ja-jp/resources/reports/2024/2024-mobile-security-index.pdf
3. Trend Micro. (2017, November 6). A misconfigured Amazon S3 exposed almost 50 thousand PII in Australia. https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/a-misconfigured-amazon-s3-exposed-almost-50-thousand-pii-in-australia
4. American Hospital Association. (2024, February 21). Change Healthcare cyberattack underscores urgent need to strengthen cyber preparedness for individual health care organizations and as a field. Retrieved June 10, 2025, from https://www.aha.org/change-healthcare-cyberattack-underscores-urgent-need-strengthen-cyber-preparedness-individual-health-care-organizations-and
5. Macaulay, T. (2024, February 20). The danger of critical infrastructure interdependency. Centre for International Governance Innovation. Retrieved June 10, 2025, from https://www.cigionline.org/articles/danger-critical-infrastructure-interdependency/
6. FirstPoint Management Resources. (2024, March 15). Analysis of top 11 cyberattacks on critical infrastructure. Retrieved June 10, 2025, from https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/
7. Columbia School of International and Public Affairs. (2022, November). NotPetya: A case study in cyber warfare. Retrieved June 10, 2025, from https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf
8. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture (NIST Special Publication No. 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
9. Tabassi, E. (2024, January 4). Insider Q&A: Small federal agency crafts standards for making AI safe, secure and trustworthy. Associated Press. Retrieved June 10, 2025, from https://apnews.com/article/84fcb42a0ba8a2b1e81deed22dd1db16
10. U.S. Department of Homeland Security. (2024, January). National Infrastructure Protection Plan: Risk management framework. Retrieved June 10, 2025, from https://www.dhs.gov/xlibrary/assets/NIPP_RiskMgmt.pdf
11. Statista. (2024, March 10). Number of cyberattacks recorded per sector. Retrieved June 10, 2025, from https://www.statista.com/chart/31985/number-of-cyber-attacks-recorded-per-sector/
12. Temple University. (2019, January). COBIT 2019 Framework: Introduction and methodology. Retrieved June 10, 2025, from https://community.mis.temple.edu/mis5203sec003spring2020/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf
13. National Institute of Standards and Technology. (2024, February). Cybersecurity and privacy white paper: NIST Cybersecurity Framework. Retrieved June 10, 2025, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Suraj Raghupathy is a Senior Cyber and Strategic Risk Consultant at Deloitte with over 6 years of experience in cyber risk consulting and management. He specializes in designing and executing third-party risk assessments, conducting vendor due diligence, and supporting enterprise compliance and threat monitoring efforts for clients across the financial services, healthcare and technology industries.

Associated ISSA Chapter: Atlanta Metro
LinkedIn Profile link: https://www.linkedin.com/in/suraj-raghupathy-iswaran/
Contact Email: suraj.raghupathy@gmail.com