Issues in Information Systems
Volume 24, Issue 4, pp. 273-281, 2023

DOI: https://doi.org/10.48009/4_iis_2023_121

The impact of unplanned system outages on critical infrastructure sectors: cybersecurity perspective

Dessu Sam, *Marymount University, dds09958@marymount.edu*
Xiang Liu, *Marymount University, xliu@marymount.edu*

Abstract

Threat actors and groups capable of launching advanced persistent threats have repeatedly breached the U.S. critical infrastructure sector's information technology systems. Although federal agencies collect and maintain valuable sensitive personal and national security information, they often fail to meet even the most basic cybersecurity standards. Insider threat (improper use) and unknown attack vectors remain the highest reported information security incidents in the federal government. Unplanned system outages with known and unknown causes are also on the rise across the industry. This study aims to investigate the impact of unplanned system outages on users, operation, network, and computer systems. The ultimate goal is to enhance our understanding of these impacts and propose effective solutions for protecting the nation's critical infrastructure. The study adopted a qualitative research method with an exploratory design. An expert and purposive sampling strategy along with a snowballing technique were employed to gather insights from 27 cybersecurity experts and field leaders. Six key themes emerged from the thematic analysis highlighting the significance of a cyberrisk strategy in bolstering the cybersecurity posture of critical national infrastructure sectors during unplanned system outages with unknown causes.

Keywords: system outages, unplanned, cyberattacks, critical infrastructure, insider threat, cyberrisk strategy

Introduction

This research focused on unplanned system outages (USOs) as opposed to planned outages (e.g., for maintenance purposes) with unknown incident reasons (UIRs). USO refers to a downtime duration in which connected computer systems and applications fail to provide services during scheduled working hours (IBM, 2021). Users are cybersecurity and information technology (IT) experts working in critical national infrastructure (CNI) sectors including enterprises, federal and local government agencies.

Data breaches and cyberattacks on CNI sectors are alarmingly on the rise. Nation states and groups capable of launching advanced persistent threats (APT) attacks have repeatedly breached enterprise and federal agency IT systems (U.S. Senate, 2019). Additionally, the healthcare system and enterprises operating within CNI sectors are facing a surge of cyberattacks, particularly ransomware attacks (Devi, 2023). Given their public presence, federal agencies' collection and retention of valuable sensitive personal and company information heightens the risk posed by unplanned outages. As a result, in its 2023 National Cybersecurity Strategy, the Biden-Harris Administration has prioritized the defense of the CNI systems and assets as the primary pillar (The White House, 2023).

Background and Literature Review

USOs with UIRs are becoming more common across the industry. However, the impact of these USOs with UIRs remains a poorly understood and researched phenomenon. At the time of writing, there are 16 federal government agencies as part of the CNI system that were considered crucial to the U.S. national security (CISA, 2023). The following subsections offer an in-depth review of the pertinent literature regarding the subject matter.

Where Internet Outages and USOs Intersect

CNI sectors including enterprises and government agencies heavily rely on robust connectivity and secure internet operations. Although research on USOs is limited, Aceto et al. (2018) conducted a comprehensive survey examining internet outrages and their impact evaluation. The ThousandEyes internet outages map provides a visual overview of the global internet outages over the last 24 hours. Internet outages appear to be an inevitable, recurring phenomenon; posing ongoing challenges in terms of analysis, detection, identification, quantification, risk assessment, and mitigation. Banerjee et al. (2015) indicated the lack of information and cooperation among major players when it comes to analyzing internet outages. Caida (2020) pointed out the absence of "near-real-time, scalable and validated methodologies and tools" to effectively detect and comprehend large-scale internet outages.

However, unlike an internet outage, USOs refer to a downtime duration in which connected computer, application or network systems fail to provide services during scheduled business hours. According to the Department of Homeland Security (DHS) (2023), system outages carry substantial security implications for work and society as the increased dependency on the internet presents new challenges for mitigation and prevention efforts. Therefore, to gain insights into the impact of USOs, and OSOs with UIRs, it is important to examine the infrastructure that supports IT in the CNI system.

Cyber-Physical Systems Security in CNI

Computer systems employed in the federal government are no longer self-contained structures; instead, they are increasingly interconnected with each other and the external networks and the internet. They form part of the human–cyber–physical realm where users play critical roles in machine-to-human, machine-to-machine, and operation and production systems. Thus, it is imperative to examine the relevance of Cyber-Physical Systems **(**CPSs) security when addressing USOs.

CPSs involve humans and complex and embedded computational, communication and control technologies to create physical systems that are capable of in-depth collaboration (Liu et al., 2017). By integrating the internet, computational and emerging technologies into physical objects and the infrastructure supporting it, CPS in fact has revolutionized human interaction with engineered systems to augment service provision. Internet-connected CPS is designed to be a smart networked system that has the potential to enhance real-time performance and operation (Al Shahrani et al., 2023). CPS is widely used in industries operated by federal agencies including energy, manufacturing, healthcare, and transportation sectors. The operation of CPS follows the Human In-The-Loop (HITL) approach, necessitating collaboration among professionals and users from diverse fields and disciplines. CPS interacts with human operators and are vulnerable to malicious codes that is generally installed and operated within human environments, hence, is safety critical.

However, within the context of HITL, both machines (automation) and humans could fail or be compromised. According to Calvert et al. (2023), while humans can potentially enhance the automation process,

they can also introduce a host of errors in systems. Consequently, components of CPS are prone to USOs and malicious attacks originating from both insider and outsider sources.

The physical process in CPS is monitored by Industrial Control Systems (ICSs), which is made up of field devices such as sensors, control devices, e.g., Programmable Logic Controllers (PLC), Supervisory Control and Data Acquisition (SCADA) workstation and Human-Machine Interface (Ahmed & Zhou, 2020). SCADA systems are software-based components within ICS. SCADA is used to monitor and control industrial processes. Therefore, in cyberspace, ICS and SCADA systems constitute crucial interconnected components of the CNI systems. Hence, a security incident in one part of ICS can affect the others in the loop.

Researchers emphasize that IT security principles of confidentiality, integrity and availability do not entirely align with the security requirements of SCADA because loss of human lives or disrupted production cannot be readily restored from backup systems, as is typically the case in traditional IT networks (Ginter, 2016). While IT security predominantly deals with data security, ICS security encompasses managing the physical world in which a large number of network devices are deployed across wide and often challenging geographic areas.

In industrial sites, the first priority is safety of the physical process. Safety refers to the well-being of personnel, the public, property, the environment and the production process (Hu et al., 2018). The second priority is the reliability of the physical process, for instance, keeping the light on. Hence, cybersecurity can be established as an essential tool to ensure the *safety and reliability* of physical processes in ICS and SCADA.

Insider Threats and Opportunities of Vulnerabilities in CNI Systems

Insider threats arise from intentional (malicious) or unintentional (also called negligent, human error or human factor) insider activities, and social engineering attacks. While unintentional insider threats (UITs) are often attributed to human error, both malicious and unintentional insider threats share many common contributing factors. According to the Carnegie Mellon University Software Engineering Institute Insider Threat program, UITs involve individuals (such as current or former employee, contractor, or business partner) who have or had legitimate access to resources. Through their actions or lack thereof, without malicious intent, UITs can cause harm or pose significant risks to data and systems (CMU SEI, 2013).

Insider threats can be accomplished through physical or cyber means. In the CPS domain, a malicious insider with access to SCADA not only possesses control over information systems but also has the capability to manipulate physical industrial sites where field sensors and actuators are located. Hence, unlike traditional IT systems, CPS of industrial sites have to deal with both cyber and physical process security. Moreover, since CPS of industrial operations span vast geographical regions, it presents unique security challenges to ICS and SCADA systems.

The introduction of emerging technologies into modern life has brought about significant transformations in the cyber-physical domain. On the other hand, although emerging technologies, such as IoTs, are broadly welcomed by Operational Technologies (OTs), businesses, and the public alike, they come with serious security challenges.

The utilization of IoT devices for data collection and sharing is on the rise. By integrating Artificial Intelligence (AI) with IoT systems, enterprises are improving their operations and business processes and automating work in real-time. In fact, enterprises are increasingly leveraging their existing IoT infrastructure to

explore new business opportunities, boost revenue, and enhance customer experience. However, lack of security considerations and improper use of IoTs has given rise to security challenges (Celik et al., 2019).

High-Profile Data Breaches and USOs

Data breaches are also associated with USOs, resulting in significant downtime and financial loss to enterprises in CNI sectors. Research shows that most of small and medium-sized businesses in the U.S. indicated cybersecurity issues as the most common causes of losses from downtime. For instance, the Coveware's (2020) analysis revealed that in 2019 the average downtime following a ransomware attack lasted 9.6 days in industries shaken by the malware, including the healthcare industry. In fact, according to IBM (2023), the healthcare industry has consistently recorded the highest average cost of data breaches for 12 consecutive years. Moreover, for managed service providers such as IT infrastructure and security enterprises, downtime costs associated with ransomware have increased by 200% year-after-year (Datto, 2019).

Methodology

This study embraced a qualitative research method. The researcher focused on capturing the professional context and lived experience of participants. The study was conducted through a survey method, where participants were presented with a set of 30 questions in semi-structured and structured formats. The survey was distributed through a secure Google form link sent from the researcher's University Google account. Due to the COVID-19 pandemic triggered changes, face-to-face interview was ruled out.

The study employed a combined strategy of purposive or expert sampling, along with a snowballing technique. By utilizing an exploratory design approach, the researcher recruited a total of twenty-seven cybersecurity and IT experts from various locations across the U.S. These experts were selected based on their extensive professional expertise and experiences related to USOs, as well as USOs with UIRs. The qualifying criteria for participation in the research required a minimum of three years of cybersecurity and/or IT work experience in CNI sectors. The researcher used their University and professional connections, as well as implemented a snowball sampling method, to identify and onboard volunteer experts. No financial incentive or compensation was offered to the participants of this study.

Purposive sampling focuses on selecting participants based on specific characteristics or expertise relevant to the research. The emphasis is not on the quantity of participants but rather on the quality and richness of the data they can provide (Saunders et al., 2018). The concept of data saturation, which signifies the point where new information ceases to emerge, is widely recognized as a methodological principle in qualitative research and serves as a benchmark for determining sample size for this study.

In accordance with the principles of Grounded Theory, the researcher examined USOs, and USOs with UIRs involving CNI sectors. The follow up communication between the participants and the researcher was facilitated via emails, phone calls and text messaging. The data was analyzed using the inductive Thematic Analysis (TA) approach where categorization of patterns, identification and integration of unifying themes, modeling and theorizing were the focus.

Guided by the six steps of TA (familiarization, coding, generating themes, reviewing themes, defining and naming themes, and write up), the researcher thoroughly examined the collected data consisting of 675 responses. A question-by-question analysis approach was employed. A total of eighty-one themes and subthemes were identified from the responses, which were subsequently consolidated into six major unifying themes. A cloud-based relational database software known as Airtable was used to analyze the data. The

research question that drove this qualitative study was: *How does implementing cyberrisk strategy help mitigate the impact of USOs with UIRs?*

Presentation of the main contribution of the paper

In the realm of cybersecurity , the term 'unknown incident reason' describes a knowledge gap. This study discovered six key unifying cybersecurity themes through the primary data collection and analysis, with potential to bridge the knowledge gap pertaining to USOs, and USOs with UIRs. Through the key themes, the study also offered valuable insights for detecting, identifying and mitigating cybersecurity incidents. The findings of this research underscore the urgent need for further investigation into the high incident rate and impact of USOs, and USOs with UIRs. Another notable finding is that over 50% of participants reported experiencing downtime resulting from USOs, highlighting the importance of addressing this issue.

This study further revealed the alienation of users from the problem-solving process, despite the fact that insider threats account for the vast majority of data and system breaches in CNI sectors, in both the public and private domain. The sheer focus on technological solutions to security threats created a knowledge gap among users and upper management as well.

Lastly, the research findings strongly support the need for a comprehensive cyberrisk strategy that fully involves all stakeholders. Such a strategy can help users and organizations build sustainable security habits to effectively mitigate cyberrisk factors.

Findings and discussion of findings

The study identified six key unifying themes involving USOs, and USOs with UIRs, as summarized below, followed by point-by-point elaborations.

- The insider threat problem
- The constantly evolving nature of cyberthreats
- Resource intensiveness of cyber tools, techniques, and professionals
- Inadequate incident response plans
- Proactive monitoring and testing of systems and applications
- Implementation of zero-trust policy

The insider threat problem

Participants were asked about cybersecurity challenges they faced in their respective positions. The majority of participants identified the insider threat problem as one of the major challenges in ensuring cybersecurity protection. Moreover, participants also expressed concerns about the lack of training or lack of sufficient knowledge among system owners, administrators, and/or security team to effectively manage technology as part of the insider problem. Furthermore, participants emphasized that an insider threat program that includes role-based and effective security awareness training programs could help

reduce human error, and ensure platforms and applications meet the needs of their users and address the constantly evolving nature of cyberthreats pertaining to USOs, and USOs with UIRs.

The constantly evolving nature of cyberthreats

The overwhelming majority of participants indicated that the constantly evolving nature of cyberthreats and the resilience of cybercriminals as serious challenges to ensuring cybersecurity protection. For example, participants pointed out various concerns, including the relentless and complicated ransomware and phishing attacks, the difficulty of dealing with active exploitable and zero-day vulnerabilities, the use of AI/ML for offensive and defensive purposes, legacy systems and the introduction of IoTs into legacy systems, and the increasing aggression of nation-state actors as security matters that keep them on their toes. Moreover, 74.1% of participants discovered security incidents resulting from insufficient monitoring and testing of systems, software and hardware failures, and legacy systems during the course of responding to USOs with UIRs.

Resource intensiveness of cyber tools, techniques, and professionals

The majority of participants included 'resource intensiveness' of cyber tools and techniques, as well as the availability and retention of cybersecurity professionals, among the major challenges they faced. Besides, change management and modernizing organizational security posture are also proved to be slow processes that require enormous resources, security awareness, and cultural shift. Participants mentioned burnout and high attrition rate among cybersecurity professionals.

Inadequate incident response plans

Responding to the question *how do you respond to USOs, and USOs with UIRs,* over seventy percent of participants indicated that they would follow established incident handling protocols, such as disaster recovery and business continuity plans. However, participants emphasized the need for additional measures to effectively address USOs with UIRs including setting up a security team that solely focuses on USOs with UIRs, employing threat modeling, and putting in place a living incident response plan. 74.1% of participants reported discovering inadequate incident handling procedures or lack of continuous testing during the course of responding to USOs with UIRs.

Proactive monitoring and testing of systems and applications

Participants indicated that to effectively respond to USOs and UIRs, the following proactive risk reducing measures should be considered: continuous and proactive monitoring of networks and systems; enforcing identity, access, patch and configuration managements; regularly conducting vulnerability assessment and penetration testing, tracking common and emerging vulnerabilities and exploits, and automation of systems. 45.6% of participants reported using a monitoring tool to proactively monitor system logs, network traffic and other performance metrics to detect and identify USOs, and USOs with UIRs.

Implementation of zero-trust policy

Participants highlighted the implementation of a zero-trust policy as a key cybersecurity tool to remediate vulnerabilities that could lead to USOs and USOs with UIRs. The recognition of the zero-trust policy by 85% of participants highlights its importance in addressing vulnerabilities and minimizing the potential for USOs and USOs with UIRs.

Implications for Research and Practice

This study identified six key themes related to USOs with UIRs. These themes inform both researchers and practitioners on specific challenges and areas that require prioritization and further examination in terms of resource allocation, cybersecurity awareness training programs, and overall cyberrisk strategy.

The revelation of insider threats as a major concern among our respondents highlights the need for organizations to strengthen their internal security measures and cultivate a cybersecurity hygiene culture. This includes implementing robust access control systems, conducting thorough background checks on employees, and providing ongoing security awareness training to prevent insider activities. Furthermore, the identification of resource intensiveness as a challenge in cybersecurity demonstrates the need for strategic allocation and prioritization of resources. Finally, a well-defined and regularly tested and updated incident response strategy is mandatory. This includes establishing clear roles and responsibilities, conducting regular simulations and drills, and fostering effective communication and collaboration among incident response teams.

In summary, practitioners can use this knowledge to inform their strategies and decision-making processes. Researchers can leverage the identified themes to guide their investigations and develop practical solutions that directly address the challenges faced by organizations. This knowledge exchange between industry, government, and academia will lead to more effective cybersecurity practices, improved resilience against cyber threats, and ultimately a safer digital environment for individuals and businesses alike.

Limitations

Limitations of the research include elements that cannot be controlled by the researcher. Several limitations were identified in this research study. First, due to confidentiality agreements, there was a slight chance that some participants from the federal government and enterprises may not have provided a complete answer, which could introduce a potential bias. Another limitation may lie in the fact that purposive sampling can be prone to researcher bias. Having recognized this fact the researcher made every effort to prevent their knowledge or assumptions from interfering with the research process. Lastly, the validity of the study may be influenced by the reliability of the software tools used in the study. To address these limitations, future studies could consider implementing measures such as obtaining more comprehensive agreements with participants to encourage openness, employing additional sampling techniques to enhance representativeness, and utilizing validated research tools to improve the robustness of the findings. Furthermore, adopting a mixed-methods approach that combines qualitative and quantitative data could provide a more comprehensive understanding of the research topic and mitigate the limitations associated with individual methods.

Conclusion

In conclusion, this study sheds light on the complex landscape of USOs and USOs with UIRs, highlighting several crucial factors that must be considered to effectively detect, identify, and mitigate their impacts. The findings emphasize the pressing need to address the insider threat problem as well as the resource-intensive nature of cybersecurity tools, techniques, and talents in combating the challenges. Organizations should adopt a living incident response plan, proactively monitor and test systems, and implement a zero-trust ecosystem. One potential future research direction could be to focus on the human factor in

cybersecurity and explore its interactions with external factors such as tools and networks. The purpose is to develop strategies and countermeasures to minimize unintentional insider threats, and ultimately the occurrence of USOs with UIR. Another research direction could be to integrate AI agents to automate monitoring, detection, and incident response processes. AI agents can be trained to analyze vast amounts of data, detect anomalies, and respond to security incidents in real-time, thereby reducing response times and enhancing overall cyber defense. We call for both researchers and practitioners to collaborate and proactively contribute towards developing innovative and resilient approach to mitigate the impact of USOs and protecting critical systems and infrastructure.

References

Aceto, G., Botta, A., Marchetta, P., Persico, V., & Pescapé, A. (2018). A comprehensive survey on internet outages. *Journal of Network and Computer Applications*, *113*, 36–63. https://doi.org/10.1016/j.jnca.2018.03.026

Ahmed, C. M., & Zhou, J. (2020). Challenges and Opportunities in CPS Security: A Physics-based Perspective. *ArXiv:2004.03178 [Cs, Eess]*. https://ui.adsabs.harvard.edu/abs/2020arXiv200403178M/abstract

Al Shahrani, A. M., Alomar, M. A., Alqahtani, K. N., Basingab, M. S., Sharma, B., & Rizwan, A. (2023). Machine Learning-Enabled Smart Industrial Automation Systems Using Internet of Things. *Sensors*, *23*(1), Article 1. https://doi.org/10.3390/s23010324

Banerjee, R., Razaghpanah, A., Chiang, L., Mishra, A., Sekar, V., Choi, Y., & Gill, P. (2015). Internet Outages, the Eyewitness Accounts: Analysis of the Outages Mailing List. In J. Mirkovic & Y. Liu (Eds.), *Passive and Active Measurement* (pp. 206–219). Springer International Publishing. https://doi.org/10.1007/978-3-319-15509-8_16

Caida. (2020, August 21). *Internet Outage Detection and Analysis (IODA)*. Center for Applied Internet Data Analysis (CAIDA). https://www.caida.org/projects/ioda/

Calvert, S. C., Johnsen, S., & George, A. (2023). *Designing Automated Vehicle and Traffic Systems towards Meaningful Human Control* (arXiv:2303.05091). arXiv. https://doi.org/10.48550/arXiv.2303.05091

Celik, Z. B., Fernandes, E., Pauley, E., Tan, G., & McDaniel, P. (2019). *Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities*. *52*(4). http://doi.org/10.1145/3333501

CISA. (2023). *Critical Infrastructure Sectors | CISA*. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

CMU SEI. (2013). *Unintentional Insider Threats: A Foundational Study* (p. 91). https://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_58748.pdf

Coveware. (2020, June 16). *Ransomware Amounts Rise Threefold*. Coveware: Ransomware Recovery First Responders. https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread

Datto. (2019). *Datto's Global State of the Channel Ransomware Report*. https://www.datto.com/resource-downloads/Datto2019_StateOfTheChannel_RansomwareReport.pdf

Devi, S. (2023). Cyber-attacks on health-care systems. *The Lancet Oncology*, *24*(4), e148. https://doi.org/10.1016/S1470-2045(23)00119-5

DHS. (2023). *Cyber Physical Systems Security (CPSSEC)*. Department of Homeland Security. https://www.dhs.gov/science-and-technology/cpssec

Ginter, A. (2016). *SCADA Security: What's broken and how to fix it*. Abterra Technologies Inc. www.ab-terra.ca

IBM. (2021). *Outage coverage*. www.ibm.com/support/knowledgecenter/ssw_ibm_i_72/rzarj/rzarjhare-qsoutage.htm

IBM. (2023, March 14). *Cost of a data breach 2022*. https://www.ibm.com/downloads/cas/3R8N1DZJ

Liu, Y., Peng, Y., Wang, B., Yao, S., & Liu, Z. (2017). *Review on Cyber-physical Systems*. https://ieeex-plore-ieee-org.proxymu.wrlc.org/stamp/stamp.jsp?tp=&arnumber=7815549

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity*, *52*(4), 1893–1907. https://doi.org/10.1007/s11135-017-0574-8

The White House. (2023, March 2). *National Cybersecurity Strategy*. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-har-ris-administration-announces-national-cybersecurity-strategy/

U.S. Senate. (2019). *FEDERAL CYBERSECURITY: AMERICA'S DATA AT RISK* (p. 99). https://www.hsgac.senate.gov/imo/media/doc/2019-06-25%20PSI%20Staff%20Report%20-%20Federal%20Cybersecurity%20Updated.pdf