Int. j. adv. multidisc. res. stud. 2023; 3(6):2905-2910

Received: 10-11-2023
Accepted: 20-12-2023

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

A Predictive Supply Chain Cyber Risk Intelligence Framework for Infrastructure and Defense Projects

Beloved D Smart
Graduate Student, Western Governors University, Salt Lake, Utah, USA

DOI: https://doi.org/10.62225/2583049X.2023.3.6.6228
Corresponding Author: **Beloved D Smart**

Abstract
The SolarWinds SUNBURST campaign, publicly disclosed in December 2020, set new standards for supply chain cyberattack sophistication by demonstrating that adversaries can compromise thousands of organizations simultaneously, including major government agencies worldwide, by corrupting a trusted software vendor's build environment and distributing a backdoored update through legitimate vendor channels. This approach bypassed substantial perimeter defenses. The Kaseya VSA attack in mid-2021 further demonstrated that advanced supply chain attack capabilities had transitioned from nation-state actors to financially motivated ransomware groups, who deployed ransomware across hundreds of managed service provider client organizations via zero-day vulnerabilities in platform software. Collectively, these campaigns revealed that conventional periodic, questionnaire-based supplier assessment approaches focused solely on first-tier suppliers, conducted annually, and reliant on self-reported security posture are inadequate for managing the dynamic supply chain cyber risk environment. This paper describes the Predictive Supply Chain Cyber Risk Intelligence (PSCRI) framework, which integrates structured threat intelligence analysis, multi-dimensional supplier risk profiling, Software Bill of Materials (SBOM) vulnerability analysis using the CycloneDX format, behavioral anomaly detection for suppliers with privileged access, and predictive risk scoring. The framework empowers infrastructure and defense project operators to continuously anticipate, assess, and mitigate third-party cyber risks. The PSCRI framework is grounded in NIST SP 800-161, DFARS 252.204-7012, NIST SP 800-171 and SP 800-172, as well as international supply chain risk management standards. This paper synthesizes supply chain security literature, regulatory requirements, and prior conceptual work on zero-trust architecture and cybersecurity governance to develop a theoretically grounded framework suitable across the defense and critical infrastructure sectors.

Keywords: Supply Chain Cyber Risk, Software Bill of Materials (SBOM: A List of all Software Components), Third-Party Risk Management, Defense Acquisition, NIST SP 800-161 (Supply Chain Risk Management Guideline), Predictive Risk Intelligence, Zero Trust (Security Model where Nothing is Trusted by Default), Software Composition Analysis (Examining Components for Vulnerabilities), DFARS (Defense Federal Acquisition Regulation Supplement), Living-off-the-Land (Use of Legitimate Software Tools for Malicious Purposes)

1. Introduction

The SolarWinds SUNBURST campaign marked a new level in supply chain attack sophistication. Experts had previously theorized such attacks but had not observed them on a scale. FireEye publicly attributed the campaign after discovering it in its environment. The attack enabled adversaries to maintain backdoor access across approximately 18,000 organizations for 9 months without detection. This was possible by exploiting the trust between software vendors and customers. As a result, attackers bypassed major investments in perimeter, endpoint, and network defenses [1, 2]. The attack's scale, stealth, and precision showed its sophistication. The SUNBURST backdoor communicated with command-and-control servers by mimicking legitimate Orion telemetry. The malware had dormancy periods and environmental checks to evade analysis and investigation. These features point to the operational security of sophisticated nation-state actors running long-term intelligence-gathering campaigns.

The Kaseya VSA attack in July 2021 demonstrated how supply chain attack methods rapidly spread to financially motivated ransomware groups following the SolarWinds campaign. Attackers exploited three zero-day vulnerabilities and previously unknown security weaknesses within the Kaseya VSA remote management platform, used by IT providers to administer client

networks remotely. This enabled managed service providers (MSPs) to deploy REvil ransomware simultaneously across approximately fifteen hundred client organizations. The event confirmed that financially motivated criminal groups now use supply chain attack techniques previously limited to nation-state actors [25, 26]. The CISA (Cybersecurity and Infrastructure Security Agency) advisory for Kaseya outlined indicators of compromise (technical evidence of malicious activity), attack paths, and recommended mitigations. The PSCRI (Public Sector Cyber Risk Index) framework incorporates this guidance into managed service provider access monitoring. It further highlighted severe downstream impacts resulting from a single MSP platform compromise, exceeding those from breaches at individual organizations. Thus, supply chain risk management requires approaches that extend beyond endpoint and network security governance.

Despite extensive records of these campaigns and ongoing CISA advisories, most infrastructure and defense project operators still use periodic, questionnaire-based supplier assessments. These assessments suffer from accuracy issues due to misaligned incentives. Suppliers may exaggerate their security posture to win business. Without third-party verification, control quality is often overstated. Annual assessment cycles create timing problems. Supplier security can change quickly, making yearly reviews outdated. These assessments also focus only on first-tier suppliers. Second- and third-tier suppliers go unassessed, the same layers involved in SolarWinds and Kaseya incidents. ENISA's 2019 threat analysis noted that supply chain attacks were becoming a preferred tactic for adversaries. The 2020 campaigns confirmed this trend on a larger scale [30, 31, 32].

2. Methodology

This paper uses a conceptual framework development methodology grounded in a systematic review of the supply chain cybersecurity literature, defense acquisition rules, and incident analysis. This approach suits a framework-development paper that aims to synthesize knowledge into a practical model rather than presenting new data. This methodology is established in cybersecurity and organizational risk research, where the complexity and variation of regulations make large, controlled studies impractical.

The literature review covered Google Scholar, IEEE Xplore, and government document repositories, including NIST's Computer Security Resource Center and the GAO Technology Audit Database. Search terms included: supply chain cyber risk, NIST 800-161, SBOM software bill of materials, CycloneDX, defense acquisition cybersecurity, DFARS 252.204-7012, third-party risk management, and predictive risk scoring. The review timeframe was from 2013 to 2021. It included the period starting with NIST SP 800-161's original release through the SolarWinds and Kaseya campaigns that led to this research. Primary sources included incident reports, congressional testimony, and interagency advisories. These documents described the threat environment for which the PSCRI framework is intended.

Inclusion criteria focused on publications addressing supply chain cyber risk management for complex infrastructure projects, including sources on software composition analysis (managing software components and their vulnerabilities), vulnerability attribution, behavioral anomaly detection for third-party access, and predictive risk scoring for supplier groups. Defense acquisition regulatory documents established compliance requirements for the PSCRI framework. Exclusion criteria removed sources focused solely on domestic commercial IT supply chain risk irrelevant to defense or critical infrastructure, as well as sources published before SolarWinds or that omitted lessons from that campaign's demonstration of nation-state attack maturity.

Framework development began by identifying gaps revealed by the SolarWinds and Kaseya attacks in supply chain risk management. Existing methods relied only on first-tier assessment, annual reviews, questionnaire-based posture, and lacked SBOM vulnerability tracking. The new framework was designed to address each gap directly. The PSCRI architecture was then evaluated for compliance with NIST SP 800-161 requirements, DFARS obligations, and real-world infrastructure project contracting constraints found in the literature. Bello *et al.*'s risk management framework for financial institutions gave a model for designing a multi-dimensional risk framework. The PSCRI methodology adapted this for the supply chain context [10].

3. Regulatory and Standards Context

3.1 NIST SP 800-161 and Federal C-SCRM

NIST SP 800-161, the authoritative federal guidance on Cybersecurity Supply Chain Risk Management, establishes a three-level governance model uniting organizational C-SCRM policies, mission, and business process supply chain security practices, and system-level acquisition controls. The publication establishes key C-SCRM practices, including supplier screening, contract-level security requirements, third-party assessments, uninterrupted monitoring of critical suppliers, and coordinated incident response across supply chain tiers. Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, establishes authorities for mandatory exclusion of transactions involving ICT products and services posing unacceptable national security risks, creating the regulatory framework for supply chain exclusion that the PSCRI framework's Supplier Risk Profile incorporates as an automated screening function [3, 6].

The CISA ICT Supply Chain Risk Management Task Force year-three report, published in 2021, provides sector-specific implementation guidance including lessons from the SolarWinds and Kaseya campaigns for supply chain security program design, confirming that the threat actor landscape for supply chain attacks expanded significantly in 2020-2021 and that the conventional assessment approaches most organizations were relying on were not calibrated to detect the attack patterns those campaigns employed [7]. DCSA supply chain risk management guidance on Foreign Ownership, Control, or Influence assessment and technology protection planning provides the contractor-level implementation requirements that the PSCRI framework operationalizes through its Supplier Intelligence Profiling component, establishing FOCI screening as a mandatory prerequisite for qualifying suppliers to defense programs involving controlled information [11].

3.2 Defense Acquisition Security Requirements

DFARS clause 252.204-7012 requires defense contractors to implement adequate security in accordance with NIST SP 800-171, report cybersecurity incidents within 72 hours, and

preserve images of compromised systems for DoD damage assessment [11]. NIST SP 800-172, published in February 2021, enhanced requirements establish advanced supply chain risk management practices for the most sensitive CUI categories, including SBOM analysis and supplier behavioral monitoring, which the PSCRI framework operationalizes at scale [22]. NIST SP 800-171 Rev. 2 specifies 110 security requirements that provide the compliance baseline for defense contractor CUI protection, with supply chain risk management requirements in the SCRM practice family, which the PSCRI framework's continuous monitoring satisfies on an ongoing basis [46].

The CycloneDX software bill of materials standard, adopted as an OWASP Foundation standard in 2021, provides machine-readable formats for complete software component inventories, allowing automated vulnerability assessment. STIX 2.1, adopted as an OASIS standard in 2021, enables structured incident characterization data to be used simultaneously for investigation documentation, government-mandated reporting, and ISAC intelligence sharing, cutting redundant characterization work that separate reporting processes for each purpose would require [21, 50].

3.3 Prior Institutional Work on Governance Integration

The integrated cybersecurity and anti-money laundering governance framework of Fadayomi, Bello, Elebe, Hammed, and Omoegun (2021) demonstrates how cross-functional financial risk governance can be unified under a shared monitoring infrastructure, with straightforward applicability to the PSCRI framework's integration of supply chain cybersecurity risk with procurement, legal, and financial risk governance functions [12]. This prior work confirms that institutional compliance requirements and supply chain risk management share sufficient structural similarities in their evidence collection, monitoring, and reporting, warranting a unified governance architecture that reduces total program costs using shared infrastructure while improving governance quality through integrated risk intelligence. The digital competence framework from prior institutional work [53] provides guidance for curriculum design to build organizational competency in supply chain risk assessment across procurement and program management workforces — a capacity development requirement that PSCRI implementations consistently identify as an important success factor.

4. Pscri Framework Architecture

4.1 Supplier Intelligence Profiling

The Supplier Intelligence Profiling component constructs and maintains comprehensive risk profiles for each supplier, integrating open-source intelligence, commercial threat intelligence, government advisories, financial health data, and historical security performance. Each profile characterizes the supplier across five dimensions. Ownership and Control Risk evaluates ultimate beneficial ownership against sanctions lists, CFIUS concern categories, and foreign adversary designation criteria. Historical Security Performance aggregates documented incidents, regulatory findings, bug bounty disclosures, and verified vulnerability data. Regulatory and Compliance Posture assesses demonstrated compliance with applicable frameworks. Financial Health evaluates supplier financial stability using credit ratings and financial statement indicators; financial distress is a documented predictor of security underinvestment as organizations cut discretionary spending to preserve operating cash. Geopolitical Risk assesses exposure in regions subject to export-control restrictions or active intelligence-collection campaigns. The National Security Commission on Artificial Intelligence's 2021 final report, which confirms state-sponsored supply chain targeting, points up the geopolitical dimension of supplier risk that the Ownership and Control component addresses [27].

The adversarial machine learning research available through 2020 documents adversary capacity to conduct sophisticated intelligence operations through supply chain relationships, including AI-augmented techniques for supply chain attack detection evasion, confirming the necessity of behavioral monitoring as a complement to ownership risk screening for identifying supply chain compromise that passes standard qualification criteria [24, 25]. The integrated cybersecurity and AML governance framework illustrates how automated compliance monitoring and anomaly detection can be sustained operationally at an institutional scale, providing a parallel governance model whose data architecture and alert management design are directly adapted from the PSCRI framework's Behavioral Anomaly Detection component [12].

4.2 SBOM Risk Analysis and Behavioral Anomaly Detection

The SBOM Risk Analysis component ingests machine-readable SBOMs in the CycloneDX format from software suppliers, maps component inventories to the National Vulnerability Database, and constructs complete dependency graphs that include transitive dependencies. For each identified vulnerability, a Contextual Vulnerability Severity score combines CVSS base metrics with operational context factors: deployment location within the network architecture (higher severity for OT or safety-critical deployments), component function (higher severity for security or authentication functions), and active exploitation intelligence from threat feeds. SBOM provenance verification verifies that the delivered software matches the declared component inventories through cryptographic hash comparisons, detecting the supply chain integrity-violation pattern exploited in the SolarWinds campaign [21].

For managed service providers and suppliers with privileged access, Behavioral Anomaly Detection monitors access patterns, data transfer behavior, authentication sequences, and API usage against baselines for 60–90-day observation periods. Privileged access sessions are monitored through PAM integration, capturing session metadata without capturing session content that might include supplier intellectual property. MITRE ATT&CK technique signatures Trusted Relationship, Supply Chain Compromise, and Valid Accounts are applied to behavioral monitoring alert streams. The insider-threat categorization framework from prior conceptual work provides the adversary-behavior taxonomy underlying the anomaly-detection rule set, recognizing that supply-chain compromises exhibit behavioral patterns structurally similar to privileged-insider threat activity from the monitoring system's perspective [32]. The Purdue Enterprise Reference Architecture provides the hierarchical network communication model within which supplier behavioral baselines are established [54].

4.3 Predictive Risk Scoring and Governance

The Predictive Risk Scoring engine integrates Supplier Intelligence Profiling scores, SBOM severity distributions, and Behavioral Anomaly Detection alert rates into a composite Predictive Supply Chain Risk Score computed as a weighted aggregate of normalized component scores. Bayesian updating refines individual supplier scores as new information accumulates. The predictive dimension extrapolates trend progressions over 30-, 60-, and 90-day horizons, enabling proactive governance decisions before risk deterioration reaches threshold levels. Threshold-based alerting generates graduated responses: Elevated range triggers heightened monitoring; Critical range mandates notification of the program security officer and SBOM re-verification; Severe range triggers acquisition-level intervention, including sourcing-alternatives analysis and potential contract suspension. Supply chain operations executives confirm that graduated alerting concentrates governance intervention on the highest-risk relationships rather than distributing attention equally across all suppliers.

PSCRI implementation follows four phases over 24 months from Tier 1 supplier profiling through a full integrated predictive scoring operation. Phase One establishes Supplier Intelligence Profiling and procurement system integration. Phase Two deploys SBOM Risk Analysis and establishes SBOM delivery requirements in new contracts. Phase Three activates Behavioral Anomaly Detection for privileged-access suppliers. Phase Four activates the full predictive scoring engine and graduated alerting protocol. The NSCAI 2021 final report's recommendations on supply chain security architecture inform the governance integration and cross-agency intelligence sharing components of Phase Four's inter-organizational coordination capabilities [27].

The PSCRI framework's threat intelligence layer integrates adversary intelligence from multiple authoritative sources covering the supply chain threat landscape. CISA advisories on software supply chain security, including post-SolarWinds guidance documenting the forensic investigation methodology and recommended mitigations, provide the specific technique-level intelligence informing the PSCRI threat model [2]. NIST SP 800-172's Enhanced Security Requirements for Critical Program Information provide the specialized supply chain security requirements applicable to defense acquisition contexts in which supply chain compromise could affect programs whose security significance exceeds the direct financial value of the affected information systems [23]. The integration of behavioral anomaly detection for supplier populations with privileged access addresses a gap in existing supply chain risk management frameworks that assess supplier security posture at assessment time but do not monitor supplier behavior continuously a gap the SolarWinds compromise exploited by using legitimate vendor update methods after initial compromise to achieve sustained, undetected access across thousands of customer networks [1, 2].

The CycloneDX SBOM analysis component of PSCRI addresses the software supply chain risk category that has grown most rapidly since the SolarWinds campaign. CycloneDX provides a standardized, machine-readable format for Software Bills of Materials that enables automated vulnerability attribution, enabling organizations to receive a new vulnerability disclosure and immediately determine which of their supplier-provided software components contain the vulnerable dependency, without manually analyzing each supplier's documentation. The integration of SBOM analysis with the PSCRI supplier risk scoring system enables CycloneDX-based vulnerability exposure to contribute directly to supplier risk scores, triggering enhanced monitoring or assessment requirements for suppliers with high-severity unpatched vulnerabilities in components deployed in the acquirer's environment. NIST SP 800-161 Rev. 1's software supply chain risk requirements establish SBOM-based vulnerability management as an expected practice for mature supply chain risk programs [10, 23, 13].

The PSCRI predictive risk scoring component applies machine-learning classification to supplier risk-profile features derived from intelligence profiling, SBOM analysis, behavioral anomaly detection, and assessment findings, generating probability estimates for supply-chain compromise events at defined time horizons. The theoretical foundation for predictive scoring in third-party risk contexts draws on research in anomaly detection and behavioral biometrics, demonstrating that behavioral patterns preceding security incidents often differ in detectable ways from normal operational patterns, enabling predictive models to identify them before incidents occur. Fadayomi *et al.*'s adaptive fraud risk scoring research provides an institutional model for real-time behavioral scoring of counterparty populations, financial fraud detection, and supply chain risk monitoring share the structural challenge of continuously evaluating the risk posture of a large population of outside entities whose compromise could impose direct financial harm on the monitoring organization [12].

The PSCRI governance integration layer connects the automated risk intelligence components to the human decision-making processes through which supply chain risk management decisions are actually made in defense and critical infrastructure organizations. Supply chain security program managers receive tiered escalation notifications calibrated to risk score thresholds, enabling appropriate management attention without alert fatigue from low-priority signals. Executive supply chain risk reports provide trend analysis across supplier populations, identifying systematic changes in risk patterns that indicate supply chain compromise campaigns before individual supplier incidents are confirmed. Supply chain security literature consistently documents that most supply chain security failures are governance failures the intelligence to identify elevated risk existed before incidents occurred, but escalation mechanisms failed to deliver that intelligence to decision-makers with authority to act before harm was done.

5. Conceptual Analysis and Conclusion

The PSCRI framework's most significant conceptual contribution is its reconceptualization of supply chain cybersecurity risk management as a continuous intelligence discipline rather than a periodic compliance function. Periodic assessment treats supplier security posture as a slowly changing property, assessable at annual intervals, when in fact it can change materially within weeks due to personnel changes, financial pressures, or active compromise. Real-time monitoring clearly models supplier posture as a continuously changing variable that demands ongoing observation, consistent with NIST SP 800-137 continuous monitoring principles extended to the supply chain domain. The framework's multidimensional risk scoring integrates dimensions of ownership risk, security

history, compliance posture, financial health, and geopolitical exposure that are typically evaluated in isolation by different organizational functions, thereby addressing the silos that enable supply chain attacks to exploit gaps between separately managed risk domains.

The PSCRI framework builds on NIST SP 800-161 supply chain risk management guidance EO 13873 CISA Task Force supply chain security implementation guidance defense acquisition security standards the INDUSTROYER and TRISIS campaign technical analyses informing OT supply chain threat scenarios earlier work on insider threat classification and integrated financial crime governance and digital education providing a governance architecture calibrated to the elevated supply chain threat environment documented in the SolarWinds and Kaseya campaigns.

Financial resilience research through integrated governance strategies documents that supply chain risk management requires the same organizational integration between risk identification, monitoring, and governance response that the PSCRI framework proposes for supply chain cybersecurity [58]. Data-driven risk evaluation models for emerging-market financial institutions demonstrate that predictive risk scoring under data scarcity is methodologically feasible, providing precedent for PSCRI's supplier risk scoring in defense supply chains, where historical incident data is similarly sparse [59, 57].

6. References

1. FireEye Inc. Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor. FireEye Threat Research, Dec 2020.
2. Cybersecurity and Infrastructure Security Agency. SolarWinds and Active Exploitation of Critical Vulnerability. Alert AA20-352A, Dec 2020.
3. Executive Order No. 13873. Securing the Information and Communications Technology and Services Supply Chain. 84 Fed. Reg. 22689, May 15, 2019.
4. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd ed. Hoboken, NJ: Wiley, 2020.
5. National Institute of Standards and Technology. Guide for Conducting Risk Assessments. NIST SP 800-30, Rev. 1, Sep 2012.
6. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. NIST, Apr 2018.
7. Cybersecurity and Infrastructure Security Agency. ICT Supply Chain Risk Management Task Force: Year Three Report. CISA, 2021.
8. Harland C, Brenchley R, Walker H. Risk in supply networks. J. Purchasing Supply Manage. 2003; 9(2):51-62.
9. Allodi C, Massacci F. Comparing vulnerability severity and exploits using case-control studies. ACM Trans. Inf. Syst. Secur. 2014; 17(1).
10. Department of Defense. Defense Federal Acquisition Regulation Supplement Clause 252.204-7012, 2020.
11. Defense Counterintelligence and Security Agency. Supply Chain Risk Management Guidance. DCSA, 2020.
12. Fadayomi O, Bello AD, Elebe O, Hammed NI, Omoegun GO. An integrated cybersecurity and anti-money laundering governance framework for financial crime prevention. Iconic Res. Eng. J. 2021; 4(11):584-600. Doi: 10.64388/IREV4I11-1713552
13. National Institute of Standards and Technology. Risk Management Framework for Information Systems and Organizations. NIST SP 800-37, Rev., Dec 2, 2018.
14. National Institute of Standards and Technology. Managing Information Security Risk. NIST SP 800-39, Mar 2011.
15. Anderson R, Moore T. The economics of information security. Science, Oct 2006; 314(5799):610-613.
16. Gordon LA, Loeb MP, Lucyshyn W. Sharing information on computer systems security: An economic analysis. J. Account. Public Policy. 2003; 22(6):461-485.
17. Elebe O. Conceptual model for insider threat classification and risk modeling in complex digital systems, 2018.
18. Elebe O. Risk-based cybersecurity assurance and data availability limitations, advances and future research opportunities, 2019.
19. Elebe O. Conceptual model for identity-centric zero trust architecture in enterprise security governance, 2021.
20. Elebe O. A conceptual end-to-end validation and user acceptance framework for enterprise systems and platform deployments, 2021.
21. OWASP Foundation. CycloneDX Software Bill of Materials (SBOM) Standard. Version 1.4, 2021.
22. National Institute of Standards and Technology. Enhanced Security Requirements for Protecting CUI. NIST SP 800-172, Feb 2021.
23. Office of Management and Budget. OMB Memorandum M-21-31, Aug 2021.
24. Cybersecurity and Infrastructure Security Agency. Compromise of U.S. Water Treatment Facility. Alert AA21-042A, Feb 2021.
25. Cybersecurity and Infrastructure Security Agency. AR21-196B: Kaseya VSA Supply-Chain Ransomware Attack. Alert, Jul 2021.
26. Weidinger L, *et al*. Ethical and social risks of harm from Language Models, arXiv:2112.04359, Dec 2021.
27. National Security Commission on Artificial Intelligence. Final Report. NSCAI, 2021.
28. Center for Internet Security. CIS Controls Version 7.1. CIS Security, Apr 2019.
29. Verizon. 2019 Data Breach Investigations Report. Verizon Communications, 2019.
30. IBM Security. Cost of a Data Breach Report 2019. IBM Corporation, Jul 2019.
31. International Organization for Standardization. Information Security Management Systems – Requirements. ISO/IEC 27001:2013, Oct 2013.
32. Cherepanov A, Lipovsky R. INDUSTROYER: Biggest Threat to Industrial Control Systems Since Stuxnet. ESET Research, Jun 2017.
33. Dragos, Inc. TRISIS Malware: Analysis of Safety System Targeted Attack. Dragos Intelligence, Dec 2017.
34. Luttgens JT, Pepe M, Mandia K. Incident Response and Computer Forensics, 3rd ed. New York: McGraw-Hill, 2014.
35. Organisation for Economic Co-operation and Development. OECD Principles on Artificial Intelligence. OECD, 2019.

36. Dempsey K, *et al*. Information Security Continuous Monitoring (ISCM) for Federal Information Systems. NIST SP 800-137, Sep 2011.
37. Johnson C, *et al*. Guide to Cyber Threat Information Sharing. NIST SP 800-150, Oct 2016.
38. Federal Information Security Modernization Act of 2014. Pub. L. No. 113-283, 128 Stat. 3073.
39. Presidential Policy Directive 21 - Critical Infrastructure Security and Resilience, Feb 12, 2013.
40. Office of Management and Budget. Managing Information as a Strategic Resource. OMB Circular A-130, Jul 2016.
41. Srinidhi B, Yan J, Bhargava HK. Effect of information security investments on firm performance. Decision Support Systems. 2015; 74:1-15.
42. Higgs JL, Pinsker RE, Smith TJ, Young GR. The relationship between board-level technology committees and reported security breaches. J. Inf. Syst. 2016; 30(3):79-98.
43. Gordon LA, Loeb MP. The economics of information security investment. ACM Trans. Inf. Syst. Secur., Nov 2002; 5(4):438-457.
44. Hubbard DW, Seiersen R. How to Measure Anything in Cybersecurity Risk. Hoboken, NJ: Wiley, 2016.
45. The Open Group. Open FAIR: Factor Analysis of Information Risk - Body of Knowledge. The Open Group Standard, 2013.
46. National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations. NIST SP 800-53, Rev., Sep 5, 2020.
47. National Institute of Standards and Technology. Protecting Controlled Unclassified Information in Nonfederal Systems. NIST SP 800-171, Rev., Feb 2, 2020.
48. OASIS CTI Technical Committee. STIX Version 2.1. OASIS Standard, Jun 2021.
49. Stouffer K, Lightman S, Pillitteri V, Abrams M, Hahn A. Guide to Industrial Control Systems (ICS) Security. NIST SP 800-82, Rev., May 2, 2015.
50. International Organization for Standardization. Risk Management – Guidelines. ISO 31000:2018, Feb 2018.
51. Bello AD, Elebe O, Hammed NI, Omoegun GO, Abutu DE. An e-learning framework for improving digital literacy and responsible technology use in primary and secondary schools. IRE Journals. 2020; 4(3). Doi: 10.64388/IREV4I3-1713776
52. Elebe O. Conceptual model for privacy-centric security engineering in digital and cloud computing systems, 2020.
53. Williams T. The Purdue Enterprise Reference Architecture. Instrumentation & Control Systems. 1994; 67(2):68-78.
54. Schneier B. Secrets and Lies: Digital Security in a Networked World. Indianapolis, IN: Wiley, 2004.
55. Akomolafe O, Agu MU. A conceptual model for enhancing internal audit quality through technology-enabled risk assessment frameworks. IRE Journals. 2018; 1(9).
56. Akomolafe O, Agu MU. Advances in financial resilience through integrated governance and compliance strategies. IRE Journals. 2019; 2(10).
57. Akomolafe O, Agu MU. A review of data-driven risk evaluation models for emerging market financial institutions. IRE Journals. 2019; 3(6).