Grenze International Journal of Engineering and Technology, June Issue

A Risk Oriented Framework and Assessment System for Organizational Digital Footprints

Azzah[1], Chahek[2], Jyolsna[3] and Roshan Lal[4]
[1-4]Amity University, Noida, India
Email: azzah.mallick@s.amity.edu, chahek.juneja@s.amity.edu, jyolsna.joemon@s.amity.edu, rchhokar@amity.edu

***Abstract*— The rapid and pervasive digitization of business processes has completely reinvented how organizations conduct operations well beyond traditional information technological boundaries to include complex, distributed ecosystems composed of cloud services, integrations with third-party providers, employee-managed domains, and vast volumes of exposed data. This ongoing evolution has grown the digital footprints of enterprises-the collective online traces that organizations leave behind-while at the same time expanding external attack surfaces, a development that increases their susceptibility to cyber threats. Traditional solutions to control these elements, such as asset inventory tools and vulnerability scanners, have been designed to document and mitigate risk. These have also been limited by their narrow, technically driven focus.**

They tend to focus on cataloging assets and evaluating technical exposures-things such as open ports or software versions-out of context for the enterprise. This paper provides an all-inclusive review of the current management literature on digital footprints and digital exposure, brought together from the realms of cybersecurity, information systems, and risk management to synthesize a more holistic understanding.

Consequently, we believe that risk-concept-based approaches centered on the holistic examination of exposed visibility and assets should be pursued; these would include probabilistic modeling and impact analysis suited to organizational contexts. In light of these findings, the paper presents a detailed digital footprint risk assessment framework with comprehensive integration of four dimensions of asset exposure: technological, informational, human, and third-party.

The multi-dimensional integration pro-motes an enterprise-oriented perspective, placing emphasis on downstream risk consequences, such as threat likelihood, impact severity, and mitigation costs, rather than mere vulnerability listings. In order to ensure practical applicability of the framework, it leverages an automated asset discovery tool that utilizes advanced scanning techniques, including machine learning-driven reconnaissance, to uncover hidden or shadow assets in com-plex enterprise environments.

The utility of the framework is demonstrated by an in-depth case study application to an anonymized mid-sized organization in the financial sector. It would identify all exposed assets in these four dimensions, outline prioritized risks-such as unmonitored third-party APIs and associated data breaches-and feed into strategic decision-making regarding remediation resource investments.

***Keywords*— Digital footprint, risk assessment, asset discovery, risk-based security, exposure management.**

Grenze ID: 01.GIJET.12.2.187_20

I. INTRODUCTION

The organizational risks related to cyber threats have, increasingly, become associated with the visibility and traceability of assets or activity on the internet. With increasingly digitized business operations, the organizational boundary of businesses had extended considerably beyond what is traditionally circumscribed as information technology infrastructure, creating distributed environments of cloud systems, third-party integrations, organizational-managed domain name spaces, and publicly accessible data assets. This, in turn, introduced new concepts of organizational digital footprint, which is defined as "the collective sum of an organization's deliberately created or accidentally generated, publicly observable, and traceable elements of its digital footprint on the open web, cloud systems, or third-party systems." With increasingly interdependent organizational infrastructure on the internet, organizational digital footprints are increasingly expansive along dimensions of size, complexity, and dynamics. The organizational digital footprint is associated with considerable organizational risks. Exposed organizational services, improperly managed cloud assets, leaked organizational credentials, or un-managed domain spaces may be readily exploited by malicious actors to selectively or improperly access sensitive organizational assets such as customer records, finan-cial accounts, or personal identifying attributes. While it is an organization's responsibility to safeguard the data they collect and process, it has become increasingly challenging to vigilantly control a distributed digital ecosystem. Also, it has been observed that organizations are able to safeguard only what they are consciously aware of and not what they actually possess as assets or are associated with in some form. Significant exposure of digital footprint risk comes from assets that are unknown, forgotten, and inadequately protected and safeguarded. Unattended subdo-mains, abandoned cloud instances, public APIs, and shadow IT projects are some of the assets that fall outside of formally protected security boundaries and create blind spots that are explored and capitalized on by attackers. While traditional network security perimeters, and in particular firewalls, continue to play a critical role in securing networks, they are inadequate in this regard regarding risks posed by assets that are exposed on a public basis, as well as valid and user-engagement-driven exposure of assets that are situation-specific and unavoidable in a manner that incurs substantial cost and damage when failure actually happens. Thus, organizations are deprived of a system-atic process for deriving meaningful enterprise risk knowledge from their external digital exposure. Solutions availa-ble for making external digital exposure more amenable for organizations emphasize discovery-capability enhance-ments for external attack surfaces. Nevertheless, currently available solutions are primarily concerned with asset identification and vulnerability identification at the technical level, without accounting for exposure transitions at the enterprise risk level.

II. BACKGROUND AND CONTRAST

The concept of digital footprints has evolved significantly alongside advancements in organizational computing envi-ronments. Initially, discussions primarily cantered on individual privacy and online traceability. However, more re-cent research, as highlighted in this paper, has shifted focus towards the organizational exposure stemming from internet-facing infrastructure, cloud services, and third-party dependencies. This evolution is driven by organizations increasingly adopting distributed digital architectures, where externally observable assets like domains, subdomains, APIs, cloud resources, and Software-as-a-Service (SaaS) platforms have become integral to their operations. While EASM offers enhanced visibility into external exposures and reduces reliance on potentially incomplete internal asset lists, the management of digital footprints largely remains focused on technical exposures and vulnerability discovery. Most external assets are treated as static inventories, with risk assessments typically based on the severity of technical findings or configuration weaknesses.

A. Related Work and Limitations of Existing Approaches

TABLE I. COMPARISON OF TRADITIONAL SECURITY RISK APPROACHES AND DIGITAL FOOTPRINT RISK PERSPECTIVE

Aspect	Traditional Security Risk Perspec-tive	Digital Footprint Risk Perspective
Asset scope	Focus on internally managed assets	Incorporates external and hidden assets
Risk posture	Reactive risk mitigation	Proactive risk identification
Assessment frequen-cy	Periodic assessments	Continuous, dynamic monitoring
Evaluation focus	Technical vulnerability severity	Enterprise and business risk impact
Decision context	Operational security teams	Strategic, governance, and ERM con-texts

Existing digital footprint and EASM tools primarily concentrate on discovering assets and weaknesses within exter-nally visible infrastructure. These tools are effective in identifying unknown domains, services, and misconfigura-tions, thereby contributing to basic security hygiene. However, their analysis is predominantly

technical, often lack-ing the contextual understanding of how these exposures translate into broader organizational or business risks.

B. Distinguishing Features of Proposed Framework

The framework presented in this study addresses the aforementioned limitations by offering a distinct approach to digital footprint risk assessment. It differentiates itself from existing methodologies in three primary ways:

- Risk-Oriented Interpretation: Unlike approaches that solely focus on technical characteristics, this framework interprets digital footprint exposure through an enterprise risk lens, evaluating assets based on their potential impact on the organization.
- Multi-Dimensional Integration: The framework integrates four crucial exposure dimensions: technologi-cal, informational, human, and third-party. This allows for a comprehensive analysis of risk across various organizational layers, moving beyond a sole focus on infrastructure.
- Dynamic Scoring Model: A dynamic scoring model is incorporated, combining exposure, exploitability, business impact, and temporal volatility. This model generates composite risk scores that continuously evolve as the external digital footprint changes, providing a more accurate and up-to-date risk profile.

III. PROPOSED FRAMEWORK AND RISK SCORING MODEL

A. Organizational Digital Footprint Risk Framework

The framework is specifically designed to overcome the limitations of discovery-centric approaches by establishing a clear connection between asset visibility and contextual risk factors that directly influence organizational impact and decision-making.

- Technological Layer: This dimension addresses risks associated with the organization's internet-facing infrastructure, including domains, subdomains, cloud resources, and other technical assets.
- Informational Layer: This layer focuses on risks related to exposed data, such as sensitive information, intellectual property, or personally identifiable information that might be publicly accessible.
- Human Layer: This dimension identifies risks stemming from the digital activities of employees, encompassing issues like shared information, credential reuse, and susceptibility to social engineering threats.
- Third-Party Layer: This encompasses risks associated with assets and services managed by third parties that are connected to or involve the organization, such as third-party APIs or cloud service providers

B. Risk Scoring Dimensions and Assessment Logic

To concretize the proposed framework, a set of interpretable and extensible scoring dimensions has been defined for evaluating digital footprint risk. The four primary dimensions are:

- Exposure (E): This represents the degree to which an asset is externally visible and discoverable. Factors contributing to a higher exposure rating include public accessibility, DNS presence, service availability, and a lack of access controls.
- Exploitability (X): This dimension quantifies the likelihood that an exposed asset can be successfully compromised by a threat actor. It considers known misconfigurations, weak authentication mechanisms, outdated services, and commonly exploited vulnerability patterns.
- Business Impact (I): This captures the potential organizational consequences of a successful compromise. Impact is contextualized based on the asset's criticality, data sensitivity, regulatory relevance, and its role within core business operations.
- Temporal Change (T): This dimension acknowledges the dynamic nature of digital footprints, capturing how frequently assets change, appear, or disappear. Newly exposed, unstable, or frequently changing as-sets are considered higher risk due to reduced visibility and increased uncertainty.

Each of these factors is ranked separately and normalized for comparison purposes before aggregation. The final digital footprint risk score is calculated by integrating these factors using a weighted logic, drawing upon established risk quantification concepts from enterprise risk management and FAIR risk models. These weights can be adjusted based on specific regulatory, operational, or threat contexts. The scoring process is inherently dynamic; as the system identifies new assets, removes old ones, or detects changes in context, risk scores are continuously adjusted to reflect the current status of the digital footprint. This dynamic approach fosters ongoing risk awareness and informs organi-zations about emerging risks. To operationalize the scoring model, each dimension is normalized on a scale between 0 and 1. The overall risk score R for an asset is computed as:

$$R = w_e E + w_x X + w_i I + w_t \mathrm{T}$$

where E, X, I, and T correspond to exposure, exploitability, business impact, and temporal volatility respectively, while w_e, w_x, w_i and w_t represent the relative weighting of each dimension.

TABLE II. RISK SCORE CRITERIA

Dimension	Score	Explanation
Exposure (E)	0.8	Public API endpoint accessible via DNS
Exploitability (X)	0.7	Weak authentication mechanism
Business Impact (I)	0.6	API interacts with operational data
Temporal Volatility (T)	0.5	Recently deployed service

Assuming equal weights $w_e = w_x = w_i = w_t = 0.25$, the resulting risk score is:

$$R = 0.25(0.8) + 0.25(0.7) + 0.25(0.6) + 0.25(0.5) = 0.65$$

This score indicates a relatively elevated risk level and therefore prioritizes the asset for remediation or further moni-toring. The scoring weights can be adjusted depending on organizational priorities, regulatory requirements, or sector-specific threat models.

C. System Architecture and Prototype Implementation

To demonstrate the feasibility and practicality of the proposed framework for digital footprint risk assessment, a prototype system has been developed. The aim of this prototype is not to deliver a production-ready system but to illustrate that the conceptual framework can be automatically implemented within a risk-aware assessment process.

From an abstract perspective, the prototype system comprises four functional modules:

- Asset Discovery Module: This module is responsible for identifying all externally visible digital assets be-longing to an organization. It automatically discovers domains, subdomains, and related internet-facing ser-vices, including those that may be unmanaged or previously unknown.
- Contextual Data Processing Component: This component processes the discovered assets, extracting rel-evant risk interpretation features. These features include, but are not limited to, risk exposure and exploita-bility characteristics, as well as business context-related attributes necessary for assessing business impact and volatility.
- Risk Scoring Stage: This stage applies the risk scoring logic outlined in the proposed framework to gener-ate a composite risk score for each identified asset. These scores are calculated by aggregating the various risk dimensions and are continuously updated as new assets are discovered or existing assets undergo changes over time.

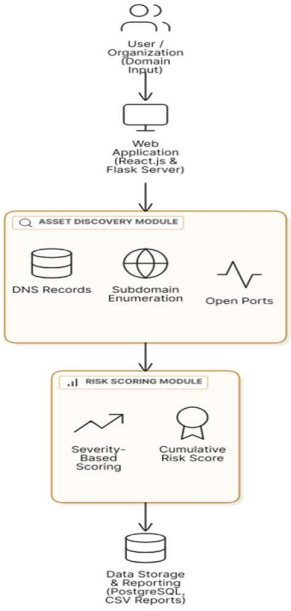

Figure 1. System architecture for the proposed digital footprint risk scoring tool

IV. Results and Discussion

The illustrative application of the proposed framework provides several key insights into the nature of digital foot-print risk within organizations and highlights the inherent weaknesses of purely discovery-driven approaches. The prototype system successfully identified a wide range of externally visible assets, including domains and subdo-mains, that were not represented in the organization's in-house asset inventories. These findings underscore the ef-fectiveness and importance of a continuous and comprehensive discovery process. Furthermore, the risk scores demonstrated dynamic shifts sponse to evolving exposure conditions, reflecting how the continuously changing ar-rangement and positioning of assets impact new exposure scenarios. The emergence of new, exposure-prone assets is recognized as a critical element of risk profiling, moving beyond an enterprise's internal interpretation of risk. Consequently, risk profiling tends to align with actual business needs rather than being constrained by an organiza-tion's internal understanding of risk as it pertains to assessment processes. This approach also facilitates improved communication by delivering aggregated risk information to risk and governance teams, replacing a fragmented col-lection of scattered technical results. In light of these observations, the findings demonstrate how a risk-oriented digital footprint analysis can support more effective prioritization and heighten awareness within the given con-straints.

Table III: Representative Assets, Risk Scores and Mitigation Strategies from Case Study

Asset Type	Example Exposure	Risk Score	Key Risk Factor	Recommended Mitigation
Public API end-point	Internet-accessible API service	0.65	Weak authentication	Implement strong authentication and API gateway controls
Subdomain ser-vice	Unmonitored subdomain	0.58	Limited monitoring	Integrate into asset inventory and monitoring systems
Third-party integration	External analytics service	0.54	Data exposure risk	Review data sharing policies and restrict permissions
Cloud service endpoint	Public storage or compute instance	0.61	Misconfiguration risk	Apply access controls and con-figuration auditing

V. Limitations

This report contains a number of assumptions that should be kept in mind when analysing its findings. First, this exemplary use of digital footprint analysis is performed on a single anonymized company and is meant to serve as a demonstration of feasibility rather than as a conclusive result with useful and meaningful statistical significance. Second, although this analysis of risk classification uses information surmised from contextual information observa-ble from the outside, this is meant to simulate a realistic operating environment within which digital footprint anal-yses are typically executed. Nonetheless, this could serve as a result that provides approximations of business impact or critical assets, when arguably a more accurate result could be achieved with a cost of reduced applicability with this use case. Thirdly, the prototype system is concerned with Internet-facing assets alone. It does not consider intra-organizational dependencies or second-order risks, which emerge after intricate connections between systems. Thus, systemic risks, or second-order risks, are not modelled as part of this framework. Finally, it may be seen that, as of now, this prototype places more weight on interpretability and viability than on accuracy. The scoring mechanism is intended to facilitate priority ranking, not measure specific amounts of either-risk or-likelihood. Future research could develop this framework along several dimensions.

VI. Conclusion

This research significantly advances our understanding of digital footprint management by introducing a comprehen-sive risk assessment framework. This framework uniquely integrates four crucial dimensions of exposure: techno-logical, informational, human, and third-party. Moving beyond a mere enumeration of vulnerabilities, it provides a holistic assessment of potential risk consequences, offering practical and actionable insights for threat prioritization and enhancing organizational resilience within an increasingly interconnected digital landscape. The utility of this framework is underscored by the automated asset discovery tool and the illustrative case study conducted with an anonymized financial organization. This application effectively demonstrated the framework's capability to uncover hidden risks, such as unmonitored third-party integrations that could lead to data breaches, and to inform strategic decision-making regarding remediation efforts. By bridging the historical gap between technical asset discovery and enterprise risk management, this approach

facilitates the proactive reduction of exposures, thereby mitigating poten-tial financial, reputational, and operational impacts. The illustrative case study further highlighted the framework's ability to identify externally visible assets and assign prioritized risk scores based on exposure, exploitability, busi-ness impact, and temporal factors. The summarized results clearly indicate that assets with even moderate technical exposure can pose significant organizational risk when contextual factors are thoroughly considered. However, it is crucial to acknowledge certain limitations pertinent to the interpretation and generalization of these findings. Primari-ly, the empirical validation was conducted on a single anonymized organization within the financial sector, serving as an illustrative example rather than a statistically significant and broadly representative sample. This design choice prioritized conceptual exemplification over wide-ranging representativeness, meaning the findings may not fully capture the nuances across diverse enterprise settings. For instance, the nature of digital footprints and risk distribu-tions can vary considerably across industries; a tech startup might exhibit higher human-linked exposures due to remote work policies, while a manufacturing firm could face greater third-party supply chain vulnerabilities. Ex-panding the framework's application to multiple organizations across various sectors and sizes would significantly enhance the generalizability of the results. Furthermore, incorporating quantitative measures, such as longitudinal risk tracking or integrating with advanced AI-driven threat intelligence, could substantially improve the framework's predictive capabilities. Longitudinal studies, specifically tracking the implementation and effectiveness of the framework over extended periods, would be invaluable in establishing its long-term impact on reducing exposure risks. While this framework is preliminary, it represents a meaningful stride toward the maturation of digital footprint studies, fostering a risk-oriented mindset that effectively aligns cybersecurity efforts with broader business objec-tives. Addressing these identified shortcomings in future work will be instrumental in developing more robust tools and methods to navigate the evolving digital threat landscape, ultimately paving the way for safer and more agile enterprises against persistent cyber threats.

REFERENCES

[1] O. Akwa, "Cyber Risk Management Using FAIR Methodology." FAIR Institute. [Online]. Available: https://www.fairinstitute.org.

[2] Z. Balog, "Using the FAIR Model for Cyber Risk Quantification." FAIR Institute. [Online]. Available: https://www.fairinstitute.org.

[3] L. Bracciale, M. Conti, F. Lauro, G. Riva, and F. Rizzo, “Detecting and preventing subdomain takeover in the Italian medical land-scape,” in IEEE Workshop Proceedings, 2020.

[4] CyberSaint, "A Practical Approach to FAIR Cyber Risk Quantification." CyberSaint. [Online]. Available: https://www.cybersaint.io.

[5] Dragos, "What Is External Attack Surface Management (EASM)." Dragos. [Online]. Available: https://www.dragos.com.

[6] Expanse Security, "What Is a Digital Footprint: Meaning, Data Types and Consequences." Expanse Security. [Online]. Availa-ble: https://www.expanse.co.

[7] FAIR Institute, "State of the Art of Operational Cyber Risk Quantification," 2021. FAIR Institute. [Online]. Availa-ble: https://www.fairinstitute.org.

[8] A. Kohnke, K. Sigler, and D. Shoemaker, “Managing the Risks of the Internet of Things,” Cybersecurity, vol. 1, no. 1, 2018.

[9] M. Howard, J. Price, H. Wang, and R. Oates, “Measuring relative attack surface in computer security,” in IEEE Symposium on Secu-rity and Privacy, 2003.

[10] T. Kim et al., “A survey of domain name system vulnerabilities and attacks,” Journal of Surveillance, Security and Safety, 2021.

[11] A. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “DDoS in the IoT: Mirai and other botnets,” Computer, vol. 50, no. 7, pp. 80–84, 2017.

[12] V. Lacidav et al., “Analysis of digital footprints associated with cybersecurity behavior,” Pattern Recognition and Artificial Intel-ligence, 2022.

[13] D. Lippa, "Digital Footprint and Its Relevance to Your Organization." Lippa. [Online]. Available: https://www.lippa.com.

[14] National Institute of Standards and Technology (NIST), "Risk Management Framework for Information Systems and Organiza-tions," NIST Special Publication 800-37 Rev. 2, 2018. [Online]. Available: https://www.nist.gov.

[15] National Institute of Standards and Technology (NIST), "Cybersecurity Framework (CSF) 2.0," 2024. [Online]. Availa-ble: https://www.nist.gov.

[16] Rapid7, "External Attack Surface Management (EASM)." Rapid7. [Online]. Available: https://www.rapid7.com.

[17] Rapid7, "What Is External Attack Surface Management (EASM)." Rapid7. [Online]. Available: https://www.rapid7.com.

[18] M. Spagnuolo et al., “Can I take your subdomain? Exploiting domain delegation misconfigurations,” in IEEE Symposium on Secu-rity and Privacy, 2015.

[19] Talos, "External Subdomain Risk: Scoring Framework for Real-Time Mitigation of Emerging Internet Threats," 2019. Talos. [Online]. Available: https://www.talosintelligence.com.
[20] Tata Communications, "External Attack Surface Management (EASM)." Tata Communications. [Online]. Availa-ble: https://www.tatacommunications.com.
[21] The Cabinet Office (UK), "Cyber Risk Quantification: Guide to FAIR Risk and Intelligence." GOV.UK. [Online]. Availa-ble: https://www.gov.uk.
[22] M. Zhang et al., "Detecting and measuring cyber risk of hosting-based domain takeovers," in Proceedings of the ACM SIGMETRICS, 2022.
[23] A. Kalra and R. L. Chhokar, "A hybrid approach using Sobel and Canny operator for digital image edge detection," in International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE) – 2016, 2016, pp. 305–310.
[24] P. S. Negi, A. Garg, and R. Lal, "Intrusion detection and prevention using honeypot network for cloud security," in 10th Interna-tional Conference on Cloud Computing, Data Science & Engineering (Confluence) – 2020, 2020, pp. 129–132.
[25] S. Pathak, H. Aggarwal, L. Sharma, and R. Lal, "Semantic vector space model for text classification using progressive learning network algorithm," in AIP Conference Proceedings, vol. 3283, no. 1, p. 040030, 2025.
[26] N. H. Rizvi, A. Sharma, A. Panesar, and R. Lal, "Analysing various CNNs for image caption generation," in Proceedings of the International Conference on Innovations in Cybersecurity and Data Science (ICICDS), pp. 651–659, 2024.
[27] R. Lal and S. K. Sharma, "Recommender process based on trust–distrust factor for signed social networks," in International Con-ference on Soft Computing for Problem-Solving, 2023, pp. 225–235.
[28] J. Dargan, A. Puri, and R. Lal, "Security and privacy in cloud/edge/fog-based schemes," in Blockchain Applications for Healthcare Informatics, 2022, pp. 351–371.
[29] P. S. Negi, R. Pawar, and R. Lal, "Vision-based real-time human–computer interaction on hand gesture recognition," in Micro-Electronics and Telecommunication Engineering: Proceedings of 3rd ICMETE.