



DATA SECURITY

CREATIVE  
COUNCIL

Workshop #1:

# Building Your Executive Dashboard



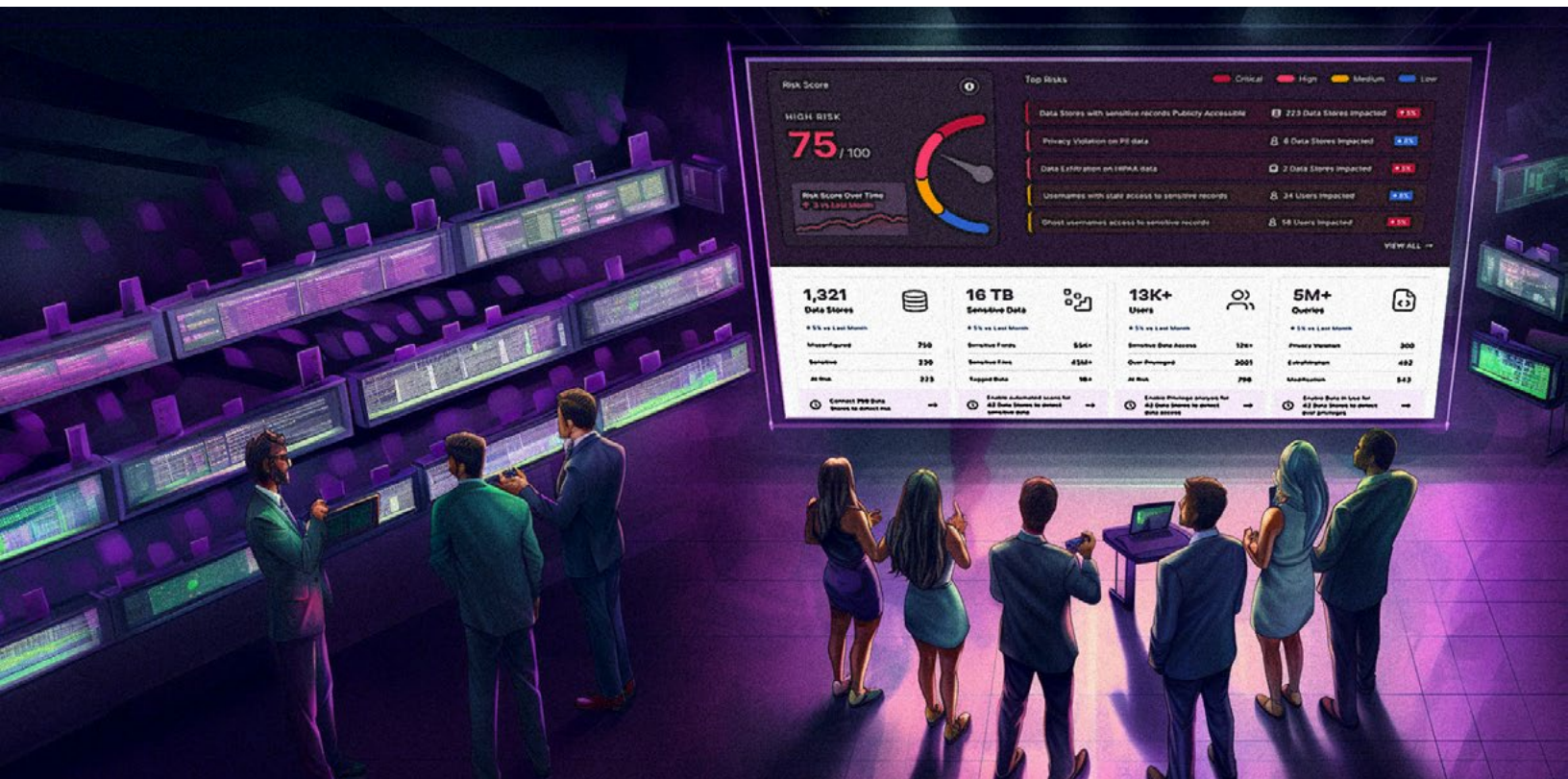
# Welcome to the first official report from the [Data Security Creative Council](#)!

The Data Security Creative Council (DSCC) is a dynamic collective of experts and leaders shaping the future of data security. This community of professionals, including but not limited to CISOs and CTOs, focuses on advancing data security through collaborative expertise, innovation, and shared knowledge. The DSCC is a hub where creativity and security intersect, driving progress and enhancing collective defenses against emerging threats.

In this shifting and evolving landscape of Data Security and Governance, the insights of seasoned professionals are invaluable. The DSCC's workshops serve as a crucial platform for knowledge exchange, bringing together experienced leaders in the field. This paper dives into the

key themes and insights from these workshops, featuring perspectives from notable Council Members: Sonali Bhagwat, Senior Director of Data Governance at Adobe; Swathi Joshi, VP of SaaS Cloud Security at Oracle; Jim Rutt, SVP and CISO at Dana Foundation, Jeff Farinich, CIO/CISO at New American Funding and Ilan Dar, CISO & SVP of Technology at AutoFi. Their collective expertise spans a range of sectors, offering a rich, multifaceted view of the intricacies of data security and governance.

Our first DSCC Workshop, "Building Your Executive Dashboard," has come to an end, and with it, some fantastic insights and actionable expertise to help you on your data security and governance journey.





DATA SECURITY  
**CREATIVE  
COUNCIL**

**Contributing  
Founding  
Members**



**Sonali Bhagwat**  
Senior Director of Data Governance  
Adobe



**Swathi Joshi**  
VP of SaaS Cloud Security  
Oracle



**Jim Rutt**  
CIO/CISO  
Dana Foundation



**Jeff Farinich**  
SVP and CISO  
New American Funding



**Ilan Dar**  
CISO & SVP of Technology  
AutoFi



**Deepti Hemwani**  
VP of Product  
Dasera



# Leadership Perspectives in Data Security

## Four Perspectives for Effective Reporting

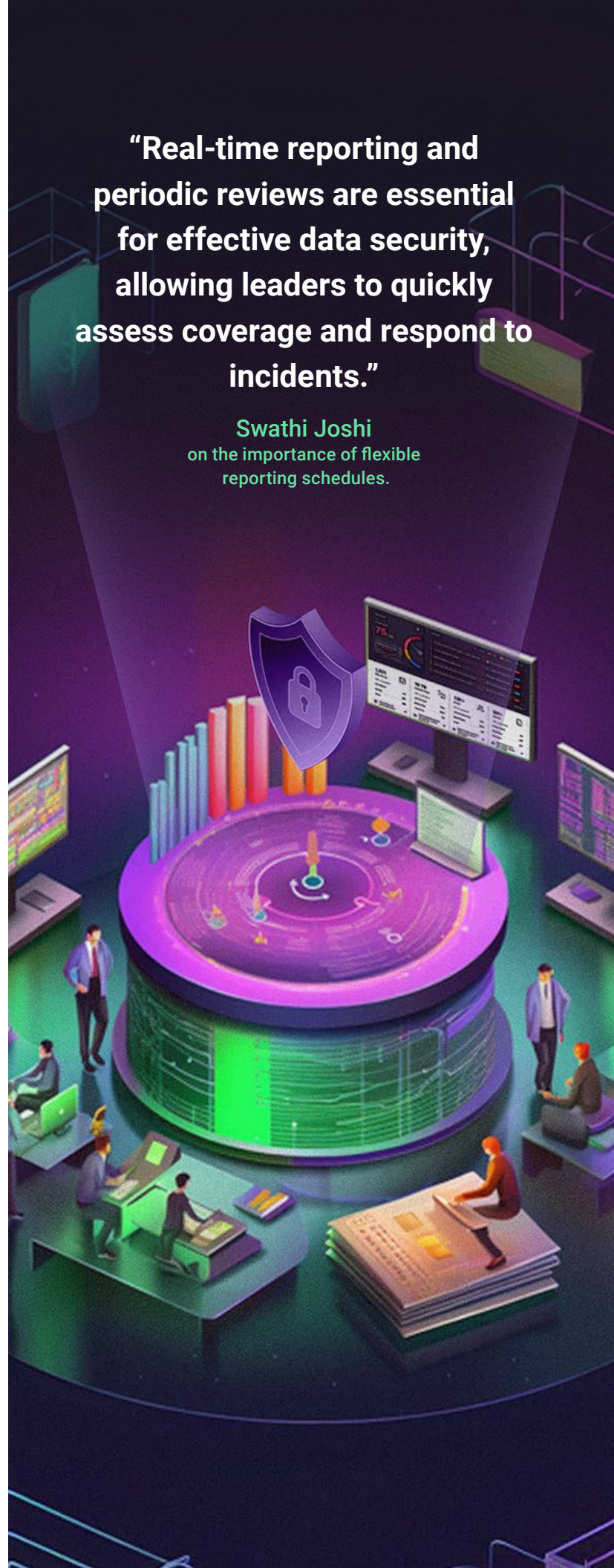
During the Data Security Creative Council workshops, Swathi Joshi, a seasoned expert from Oracle, introduced a compelling framework for data security reporting. Her approach underscores the importance of addressing four perspectives:

1. **Upwards to management**
2. **Sideways to stakeholders**
3. **Inward to the team**
4. **Downwards to support staff**

This quadrilateral reporting model ensures the data security narrative resonates across all organizational strata. By recognizing and addressing these diverse audiences, her framework ensures that each group receives tailored, relevant information. This method not only fosters a deeper understanding and alignment within teams but also enhances decision-making efficacy, thereby strengthening the overall data security posture of the organization.

**“Real-time reporting and periodic reviews are essential for effective data security, allowing leaders to quickly assess coverage and respond to incidents.”**

**Swathi Joshi**  
on the importance of flexible reporting schedules.





## Operational Dynamics and Challenges

### Understanding Diverse Reporting Scenarios

In the workshops, Swathi Joshi from Oracle illuminated the diverse landscapes of data security reporting. She emphasized how different scenarios, from incident response to real-time risk dashboards and daily snapshots of data states, demand distinct reporting approaches. A standout concept she introduced was “herd immunity” in the context of security consulting. This innovative idea highlights the power of shared intelligence and experiences within the security community. By pooling knowledge and insights from various sources, organizations can significantly bolster their security frameworks, mirroring the collective defense seen in herd immunity. This approach underlines the value of collaborative insights in navigating complex security landscapes and proactively addressing potential threats

### The Desired Format of Reporting

A key theme of the workshop emerged around the preferred formats for reporting data security and governance. Insights from Jim Rutt, SVP and CISO at Dana Foundation, and Jeff Farinich, CIO/CISO at New American Funding, shed light on leaders’ preferred reporting formats. A combination of high-level presentations and

**“Beyond traditional metrics, focusing on top risk areas and providing actionable insights is more effective than numerical scores in guiding executive decisions on data security.”**

**Sonali Bhagwat**

*on evolving approaches to security metrics.*

detailed Excel reports is favored, providing a holistic view that includes actionable insights and detailed analysis. Most council members strongly preferred reports that present data and provide clear trends and actionable insights. This approach facilitates better decision-making, particularly when benchmarked against industry standards. Bhagwat offered a notable example from the workshop: Adobe’s innovative reporting approach. They have shifted focus from relying on numerical security scores to emphasizing identifying top-risk areas. This method highlights the critical areas requiring immediate attention and investment, offering a more strategic and effective way of addressing data security concerns. This

**“Customizable dashboards with industry benchmarks empower leaders to make informed decisions, emphasizing the need for reports that are both comprehensive and adaptable.”**

**Jeff Farinich**

on reporting preferences for data security and governance.

evolution in reporting underscores the importance of actionable insights, moving beyond mere data points to provide meaningful and impactful information.

### **Challenges in Data Sharing with Business Partners**

Another focal point of the workshop was the complexities of data sharing with business partners. Experts like Sonali Bhagwat and Swathi Joshi shared strategies to navigate challenges, such as ensuring comprehensive coverage and managing efficient scan times. They discussed implementing robust data governance policies and using advanced encryption techniques for data shared with partners. Real-world examples included case studies from the healthcare sector, demonstrating effective data-sharing strategies while adhering to stringent compliance standards like HIPAA. One example highlighted a healthcare provider implementing a secure data exchange platform, ensuring that patient data shared with research partners was de-identified and encrypted. Another case involved a hospital network that

utilized advanced data classification tools to automatically identify and control sensitive health information before sharing it with insurance providers. These examples showcased the importance of compliance in data sharing and the innovative use of technology to maintain data security in complex healthcare ecosystems.

There were also case studies from the tech industry. One instance involved a tech giant collaborating with a network of smaller startups. They established a centralized data repository with strict access controls and real-time monitoring to manage data sharing efficiently, ensuring data integrity and security across different entities. Another case focused on a software company that shared data with external development teams. They used API-based integrations with robust authentication and logging systems to monitor data access and usage, thus maintaining a high level of security while facilitating necessary data exchange for collaborative development. These strategies and examples highlighted the necessity of custom solutions tailored to industry-specific requirements, ensuring data integrity and efficient collaboration.



## Strategic Approaches and Innovations

---

### Industry-Specific Benchmarking and Metrics

The significance of industry-specific benchmarking and metrics in data security strategies was a key focus of the Data Security Creative Council. Members discussed how different industries, like finance and healthcare, prioritize distinct metrics such as encryption scores or sensitive records count, reflecting their unique regulatory and risk landscapes. The council emphasized the need for tailored benchmarks and metrics, enabling organizations to effectively measure and enhance data health. This approach ensures that data security strategies align with industry-specific compliance requirements, offering a comprehensive and targeted framework for data governance. This industry-focused perspective is crucial for organizations to develop robust, relevant, and compliant data security measures.

---

### Revolutionizing Security Scores

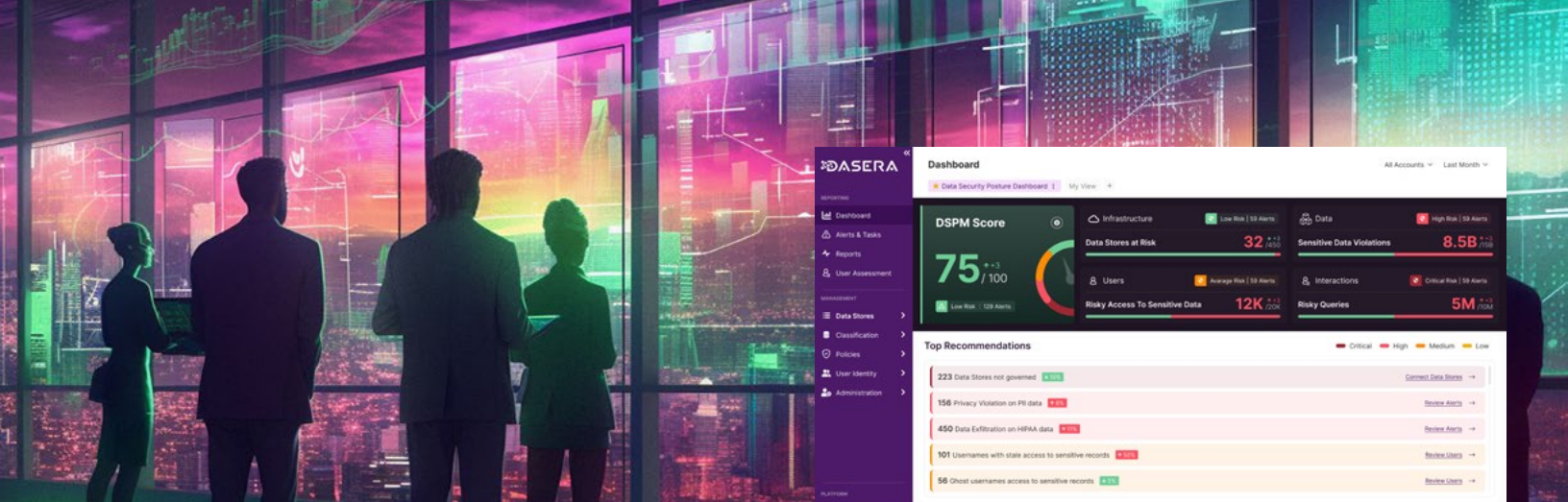
In the workshops, a nuanced perspective on security scoring emerged, highlighting the limitations of traditional numerical systems. Instead, a strategic approach was proposed that zeroes in on each executive's top three risk areas. This method, aimed at enhancing clarity

and immediacy in decision-making, allows for a focused allocation of resources towards the most pressing security concerns. By prioritizing these critical vulnerabilities, executives can formulate targeted strategies for mitigation and investment, leading to a more effective and efficient response to security threats. This shift underscores a growing trend in data security management towards tailored, actionable intelligence over generic metrics.

---

### The Importance of Flexible Time Ranges in Reporting

During the workshop, Ilan Dar emphasized the critical need for flexible reporting timelines in data security. Drawing from his rich background at AutoFi, he illustrated how the efficacy of reporting is significantly enhanced when it adapts to various time scales. This flexibility ranges from providing real-time updates during critical incidents to facilitating comprehensive overviews in periodic strategic reviews. His insights underscored the reality that different situations demand different reporting cadences, and the ability to tailor this timing is vital in ensuring that reports are informative, timely, and contextually relevant.

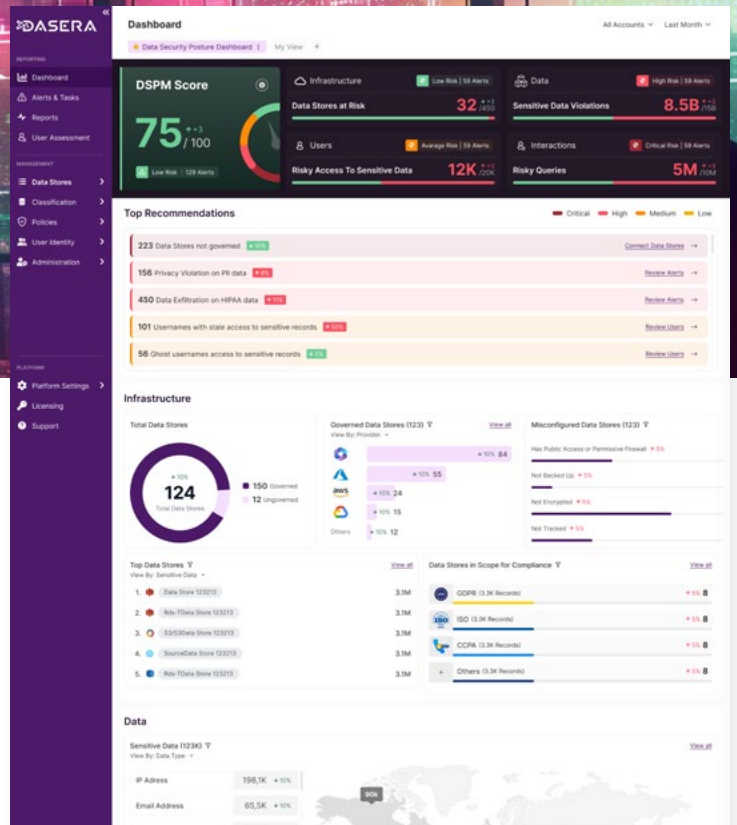


# Future Directions and Synthesis

## Workshop Synthesis and Future Plans

Reflecting on our dynamic discussions during the Data Security Creative Council workshops, we explored a range of critical themes: effective reporting from multiple perspectives, diverse reporting scenarios tailored to different situations, the importance of flexible time ranges in reporting, and the need for industry-specific benchmarking and metrics. These insights, contributed by esteemed members like Sonali Bhagwat, Swathi Joshi, and Ilan Dar, have paved the way for enhanced understanding and approaches to data security and governance.

As we look to the future, the DSCC remains committed to fostering innovation and collaboration in data security. Plans for future events are already in the pipeline, focusing on expanding our dialogue and collaborative efforts. These upcoming sessions aim to engage the data security community further, fostering



Dashboard design influenced by the Data Security Creative Council.

an environment where collective wisdom and shared experiences lead to groundbreaking solutions and strategies. Stay tuned for more updates and opportunities to participate in this transformative journey in data security.

Our first workshop series has been a milestone in collaborative data security excellence. The insights and strategies shared will be valuable for organizations seeking to strengthen their data security and governance frameworks. Stay engaged with the DSCC for future updates and collaborative opportunities in this ever-evolving field.



## Interested in the latest in data security and governance?

For insights from the [Data Security Creative Council](#) Workshop, details about our founding members, or to join our dynamic community of data and security professionals, [click here](#). Don't miss out on our upcoming content, webinars, workshops, and events designed to keep you at the forefront of data security innovation.