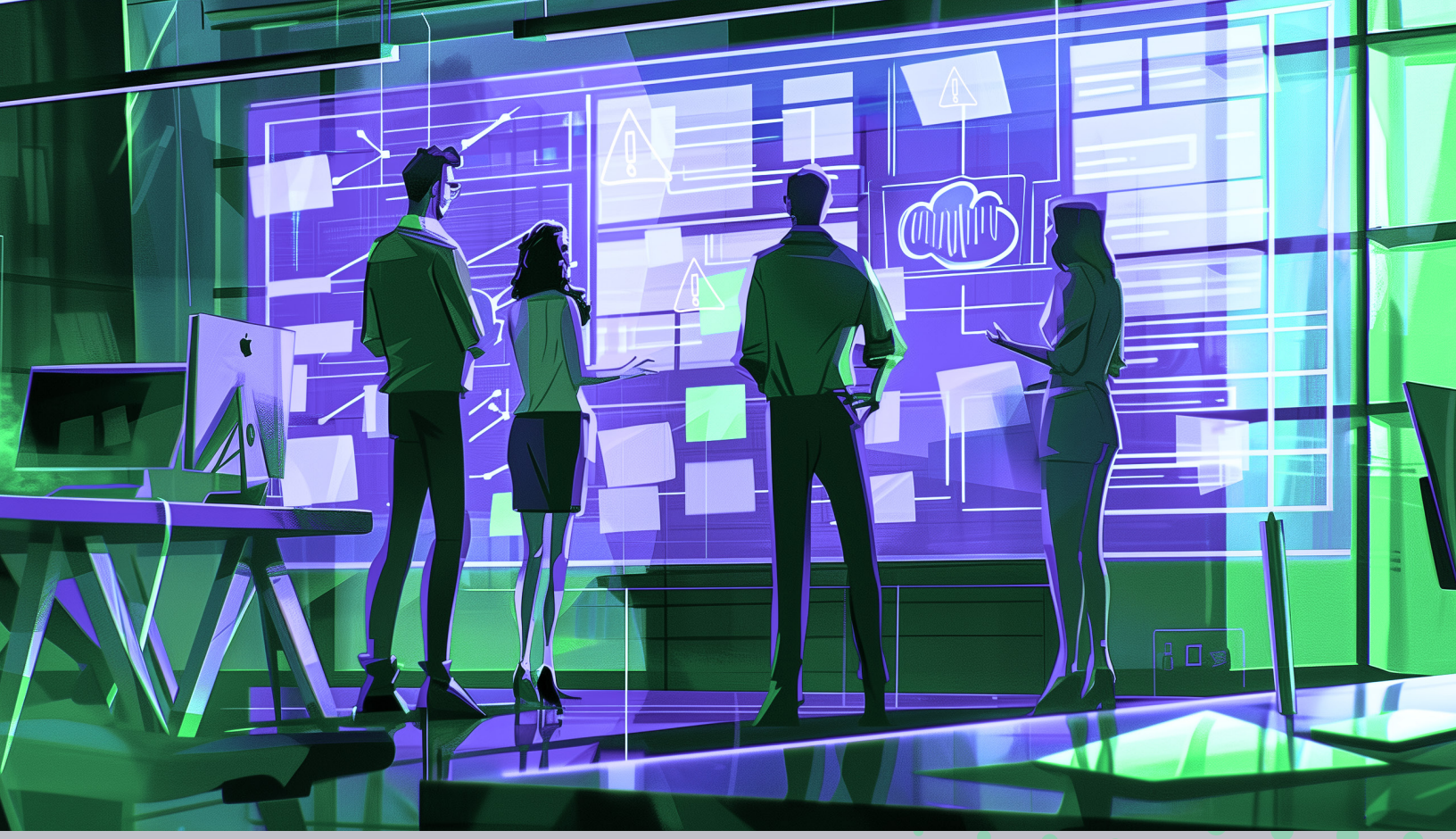

Workshop #3:

Building a Data Protection Strategy

Insights from Industry Leaders

DATA SECURITY CREATIVE COUNCIL

DATA SECURITY
CREATIVE COUNCIL

Workshop #3

Building a Data Protection Strategy

Data protection has become a critical priority for organizations of all sizes. As data breaches and cyber threats continue, safeguarding sensitive information is essential to comply with regulatory requirements and maintain trust and credibility with customers and stakeholders. Effective data protection strategies are vital in mitigating risks, preventing data loss, and ensuring the integrity and confidentiality of valuable data assets.

In a collaborative effort, we organized a workshop with leading security and data professionals to discuss the intricacies of building robust data protection programs. The objective was to pool insights, exchange experiences, and pinpoint best practices in formulating comprehensive data protection strategies. This white paper encapsulates the collective wisdom from that workshop, serving as a practical guide to assist organizations in developing and enhancing their data protection programs. Leveraging the perspectives and expertise of industry leaders, we strive to offer actionable recommendations and innovative approaches to navigating the ever-changing terrain of data security.

DATA SECURITY
CREATIVE COUNCIL
Contributing Members

Jim Rutt
CISO
The Dana Foundation

Mahesh Ayyala
CISO and Chief Data Protection Officer
Hidden Road Inc.

Matt King
Security and Data Officer
Belcan

Karen Lopez
Data Evangelist
Infoadvisors

Venkat Valleru
Principal Information Security and Compliance Engineer
Informatica

Establishing an Active Data Protection Program

Primary Objectives

The primary objectives of an active data protection program is to safeguard sensitive data and ensure regulatory compliance. This involves implementing comprehensive measures to protect data from unauthorized access, breaches, and other security threats. Ensuring compliance with relevant data protection regulations is also vital, helping organizations avoid legal penalties and maintain stakeholder trust.

Key Stakeholders

An effective data protection program requires the involvement of various stakeholders across the organization. Key stakeholders include:

- **Board of Directors:** Providing oversight and ensuring data protection is a strategic priority.
- **Executive Committee:** Leading the implementation and integration of data protection measures into business processes.
- **Steering Committee:** Coordinating efforts across departments and ensuring alignment with organizational goals.
- **Data Owners:** Individuals responsible for managing and safeguarding specific data sets, ensuring compliance with policies and procedures.

> **"Primary objectives include regulatory compliance, data governance, protection of sensitive information, and maintaining good data quality and hygiene."**
>
> **—Jim Rutt, CISO, The Dana Foundation**

Program Components

To build a robust data protection program, organizations should focus on the following components:

- **Education:** Regular training sessions to increase awareness about data protection policies and best practices among employees at all levels.
- **Workshops:** Interactive sessions to develop practical skills and understanding of data protection tools and techniques.
- **Data Repository Reviews:** Conducting thorough assessments of data repositories to identify vulnerabilities and ensure they are secure.
- **Monitoring Controls:** Implementing continuous monitoring systems to detect and respond to potential threats in real time.

Focusing on these components and involving key stakeholders can help organizations establish a strong foundation for their data protection program. This proactive approach enhances security and builds a culture of data stewardship and accountability within the organization.

Elements of a Data Protection Program

Layers of Protection

A comprehensive data protection program safeguards sensitive information using multiple security measures. These layers work together to ensure that data remains secure and accessible only to authorized individuals.

- **Access Requests and Data Encryption:** Matt King from Belcan emphasized that implementing least privilege principles minimizes data access. Organizations can significantly reduce the risk of unauthorized data exposure by granting access only to those who need it for their roles. Additionally, encrypting data at rest and in transit ensures that even if data is intercepted, it remains unreadable to unauthorized parties.
- **Network Segmentation and Data Loss Prevention (DLP):** Mahesh Ayyala from Hidden Road, Inc. discussed network segmentation (isolation segments of network), network egress monitoring, and data loss prevention tools as some of the techniques for containing potential breaches.

> "The data security program should be focused on protecting crown jewels, access, availability, and compliance."
>
> **— Mahesh Ayyala**
> **CISO and Chief Data Protection Officer**
> **Hidden Road Inc.**

Components

Organizations must focus on several key components to build a data protection program. These components form the foundation of a robust data protection strategy:

- **Backup, Recovery, and Testing:** Regularly backing up data and testing recovery procedures ensure that organizations can quickly restore data during a loss or breach. This component is critical for maintaining business continuity and minimizing downtime.
- **Data Inventory and Classification:** Maintaining an accurate inventory of all data assets and classifying them based on sensitivity helps prioritize protection efforts. Venkat Valleru pointed out that understanding what data exists and where it is stored enables organizations to implement appropriate security measures.
- **Data Policy, Standards, and Governance:** Clear data policies, standards, and governance frameworks are essential for consistent data protection practices. These guidelines ensure all employees understand their roles and responsibilities in safeguarding data.
- **Gap Assessments and Remediation:** Conducting regular assessments to identify gaps in data protection measures allows organizations to address vulnerabilities proactively. Implementing remediation plans helps close these gaps and strengthen overall security.

By integrating these key elements into their data protection programs, organizations can create a layered defense strategy that effectively safeguards sensitive information and ensures compliance with regulatory requirements.

Challenges in Data Protection

Implementing a data protection program has its challenges. Organizations often face several common obstacles that can hinder their efforts to safeguard sensitive information:

- **Educating and Upskilling Staff on Data Ownership and Responsibilities:** It is crucial to ensure all employees understand their roles in data protection. This involves continuous training and educating staff about best practices and emerging threats. Matt King noted that timing and engagement can be significant hurdles, particularly with team members' availability.
- **Communicating Data-Centric Perspectives to Legal Teams:** Jim Rutt pointed out that bridging the gap between technical data protection measures and legal requirements can be challenging. Legal teams need to understand the data-centric aspects of protection to provide accurate and relevant guidance.
- **Keeping Up with Evolving Regulations:** Data protection regulations continually change, and organizations must stay current to remain compliant. This requires ongoing monitoring and adaptation of policies and procedures.
- **Ensuring Comprehensive Data Classification and Monitoring:** Properly classifying data and implementing robust monitoring systems are essential for data protection. However, this can be a complex and resource-intensive process.

Specific Issues

In addition to these common challenges, organizations often encounter specific issues that require targeted solutions:

- **Limited Data Inventory and Classification Enforcement:** Maintaining an accurate and up-to-date inventory of all data assets can be difficult, especially in large organizations. Another significant challenge is ensuring that data is consistently classified and protected according to sensitivity.
- **Lack of Data Flows and Understanding of Regulatory Compliance:** Understanding how data flows within the organization and ensuring that all processes comply with relevant regulations is critical. This requires a deep understanding of data protection's technical and legal aspects. Karen Lopez noted the importance of understanding data flows and ensuring compliance with regulatory requirements, stating that many organizations need help with data privacy and security nuances, often leaving gaps in their protection strategies.

Addressing these challenges requires a comprehensive approach that combines education, communication, and continuous improvement. By acknowledging and tackling these obstacles head-on, organizations can strengthen their data protection programs and better safeguard their valuable information assets.

> "Timing and engagement have been the biggest challenges, particularly as it relates to other team members for other teams and their availability. We run a very lean IT shop, so everything must be prioritized."
>
> **— Matt King, Security and Data Officer Belcan**

Measuring Success

Key Performance Indicators (KPIs)

To determine the effectiveness of a data protection program, organizations must establish clear metrics for success. Key Performance Indicators (KPIs) provide a quantifiable means to evaluate the program's impact and ensure it meets its objectives. Essential KPIs include:

- **Tracking Regulatory Compliance Metrics:** Regularly measuring compliance with data protection regulations helps ensure that the organization adheres to legal requirements. This includes monitoring adherence to GDPR, CPRA, PCI-DSS, HIPAA, and other relevant frameworks.
- **Monitoring for Data Breaches and Policy Adherence:** Continuous monitoring and assessing adherence to data protection policies are critical. This involves tracking incidents of unauthorized access, data leaks, and policy violations to identify areas for improvement.

Continuous Improvement:

Achieving success in data protection is not a one-time effort; it requires ongoing evaluation and enhancement. Continuous improvement processes help organizations adapt to new threats, technologies, and regulatory changes. Strategies for continuous improvement include:

- **Regular Assessments:** Regular assessments of the data protection program help identify gaps and areas for enhancement. These assessments should cover all aspects of data protection, including technical controls, policies, and employee training.
- **Third-Party Reviews:** Engaging third-party experts to review the data protection program provides an external perspective and ensures objectivity. These reviews uncover issues that internal teams might overlook and provide recommendations for improvement.

By focusing on these KPIs and committing to continuous improvement, organizations can ensure that their data protection programs remain effective and responsive to evolving challenges. Regular assessments and third-party reviews are crucial in maintaining high data security and compliance standards, safeguarding sensitive information and enhancing organizational resilience.

Best Practices for Data Protection

Implementing best practices is essential for creating a robust data protection program. These practices help ensure that data is safeguarded effectively and that the organization is prepared to respond to potential threats. Standard practices include:

- **Implementing Robust Backup and Recovery Procedures:** Regularly backing up data and having reliable recovery processes are critical for ensuring business continuity. This ensures that data can be restored quickly during a loss or breach, minimizing downtime and impact.
- **Comprehensive Data Inventories and Classification:** Maintaining a detailed inventory of all data assets and classifying them based on sensitivity levels helps prioritize protection efforts. Knowing where data resides and its importance enables organizations to apply appropriate security measures.
- **Continuous Education and Training for All Stakeholders:** Regular training and awareness programs for employees at all levels help reinforce the importance of data protection. It is crucial for a security culture to educate staff about best practices, potential threats, and their roles in safeguarding data.
- **Integration of Advanced Monitoring Tools and AI/ML Technologies:** Leveraging these tools and technologies enhances the organization's ability to detect and respond to threats in real-time. These tools provide insights into data usage patterns, identify anomalies, and automate routine security tasks.

Areas for Improvement

While many organizations implement standard best practices, there are still areas that require improvement to achieve optimal data protection:

- **Enhancing Data Literacy Among Compliance and Data Professionals:** It is essential to increase the data literacy of compliance and data professionals. This involves providing training on data protection regulations, data handling best practices, and the technical aspects of data security. Improved literacy helps these professionals effectively collaborate and implement data protection measures.
- **Bridging Gaps Between Security and Compliance Teams:** Effective data protection requires seamless collaboration between security and compliance teams. Bridging gaps between these teams involves fostering communication, aligning goals, and ensuring that both groups understand the importance of their roles. This alignment helps create a unified approach to data protection and compliance.

By following these best practices and addressing areas for improvement, organizations can strengthen their data protection programs and ensure they are well-equipped to handle current and future challenges. Embedding best practices into the organization's culture and continuously seeking opportunities for enhancement are essential in maintaining a resilient and effective data protection strategy.

> "A best practice is embedding data catalogs into all products and ensuring a central data system for governance and security."
>
> — Karen Lopez, Data Evangelist, Infoadvisors

Impact of AI/ML on Data Protection Programs

Integrating artificial intelligence (AI) and machine learning (ML) technologies has brought significant advancements to data protection programs. These technologies enhance the ability to safeguard data by providing advanced capabilities that were previously unattainable. Key enhancements include:

- **Anomaly Detection and Data Classification:** AI/ML algorithms can identify unusual patterns and behaviors in data usage that may indicate a security threat. These technologies can detect real-time anomalies by continuously analyzing data, allowing quicker responses to potential breaches. Additionally, AI/ML can automate data classification, ensuring data is consistently categorized according to sensitivity.
- Predicting and Preventing Data Breaches: AI/ML technologies can analyze vast amounts of data to predict potential security incidents before they occur. By identifying patterns and trends that precede breaches, these tools can help organizations take proactive measures to prevent data breaches.
- Automating Routine Tasks and Improving Monitoring Capabilities: AI/ML can automate routine data protection tasks, such as monitoring for policy compliance and detecting unauthorized access. This automation enhances efficiency and ensures these tasks are performed consistently and accurately.

Challenge:

While AI/ML technologies offer substantial benefits, they also introduce new challenges that organizations must address to ensure proper data protection:

- Ensuring that AI/ML Tools Do Not Replace Human Oversight and Responsibility: One of the primary challenges is ensuring that AI/ML tools complement rather than replace human oversight. While these technologies can automate many tasks, human judgment and decision-making are crucial in interpreting the results and taking appropriate actions. Maintaining a balance where AI/ML tools assist human operators is essential without undermining their responsibility and accountability.

By leveraging AI/ML technologies, organizations can significantly enhance their data protection programs. These technologies provide powerful tools for detecting threats, predicting breaches, automating routine tasks, and improving overall security posture. However, addressing the challenges associated with AI/ML integration is crucial to ensure these tools are used responsibly and complement human oversight in data protection efforts.

> **"Identifying where the actual data is and maintaining accurate data inventory are ongoing challenges. Integrating AI/ML has helped us automate some of these tasks, but it still requires significant human oversight and intervention."**
>
> **—Venkat Valleru, Principal Information Security and Compliance Engineer, Informatica**

Moving Forward: Strengthening Data Protection Programs

The workshop provided insights from leading security and data professionals, highlighting the complexities and critical components of building robust data protection programs. Through detailed discussions and shared experiences, several takeaways emerged:

1. **Establishing an Active Data Protection Program**: To protect sensitive data and ensure regulatory compliance, it is essential to have clear objectives, involve key stakeholders, and implement comprehensive program components.
2. **Elements of a Data Protection Program:** Effective programs incorporate multiple layers of protection, including access requests, data encryption, network segmentation, and data loss prevention. Essential components such as backup, recovery, data inventory, classification, and continuous monitoring are vital for success.
3. **Data Protection Challenges:** Common challenges include educating and upskilling staff, communicating data-centric perspectives to legal teams, keeping up with evolving regulations, and ensuring comprehensive data classification. Addressing these challenges requires a strategic and continuous effort.
4. **Measuring Success:** Establishing key performance indicators (KPIs) and committing to continuous improvement through regular assessments and third-party reviews are critical for maintaining the effectiveness of data protection programs.
5. **Best Practices for Data Protection:** Implementing robust backup and recovery procedures, maintaining comprehensive data inventories, continuous education and training, and integrating advanced monitoring tools are essential best practices. Additionally, improving data literacy and bridging gaps between security and compliance teams are crucial areas for enhancement.
6. **Impact of AI/ML on Data Protection Programs:** AI/ML technologies provide significant enhancements in anomaly detection, data classification, predicting and preventing data breaches, and automating routine tasks. However, it is essential to ensure these tools do not replace human oversight and responsibility.

Emphasis on the Importance of a Well-structured Data Protection Program

A well-structured data protection program is a regulatory requirement and a strategic necessity for safeguarding an organization's most valuable assets. Effective data protection programs enhance security, ensure compliance, and build trust with customers and stakeholders. Organizations must prioritize developing and continuously improving their data protection strategies to stay ahead of evolving threats.

In the face of constantly changing threats and regulations, organizations must remain vigilant and proactive in their data protection efforts. This includes continuously evaluating and enhancing their data protection programs, staying informed about emerging technologies and best practices, and fostering a culture of security within the organization. By committing to these principles, organizations can better protect their data, maintain compliance, and ensure long-term success in the digital landscape.

For those looking to dive deeper into the complexities of data protection or to engage further with leading experts in the field, we invite you to explore more resources or request an invitation to participate in the DSCC. Whether you're seeking guidance on specific compliance challenges or wish to contribute to ongoing discussions with your insights, the DSCC is an invaluable resource.

Visit Dasera's Data Security Creative Council page for more information about past workshops and upcoming events and how you can join this dynamic community. Join us in shaping the future of data security and compliance by sharing your experiences and learning from seasoned professionals in the 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.