cyberhaven

Data Protection Checklist:

A Blueprint for Enabling DLP

Before Building Your Program

Build cross-functional relationships

Identify stakeholders: Who are your partners?

□ **IT** will generally be responsible for deploying security controls and monitoring employee behavior, so it's imperative to work closely

□ **Data stewards** are employees across multiple departments who are responsible for configuring the applications their departments use to carry out their work (i.e., a Salesforce Admin)

□ **Data owners** are employees are employees and end-users to whom data may belong because they work in the department that generates that data or because they have a hand in generating, modifying, and sharing this data.

□ **Legal, risk, and compliance** will be critical to work with to understand how to reduce legal liability and handle responsibilities during a breach or incident

□ **C-suite** and business leadership can provide guidance on how security can enable the business

□ **Roles and people specific to your organization.** You know your organization best; there might be roles or individuals you wish to work closely with to ensure the success of your program. These could be champions of security or others who are influential within the organization

Meet regularly with stakeholders

□ Establish communication channels where you'll engage stakeholders, whether this be recurring meetings, Slack channels, etc.

□ Understand the needs of these stakeholders so that you can enable them to help make your DLP program a success

□ Keep them abreast of security developments, including the initiative of building a DLP program

□ Leverage their knowledge of existing processes to begin to inform the fundamentals of your program

Understand the business

Study the business

□ Understand both immediate and long-term business objectives

□ Identify areas where security can enable these objectives so you can build your program around them

□ Conduct business process reviews to learn more about how the organization functions to avoid negative productivity impacts when rolling out your program

Section 2

Building the Program

Implement program objectives

Leverage a security framework to inform the policies, processes, and controls of your DLP program

□ Conduct research, talk with peers, and attend industry conferences to learn more about relevant differences between security frameworks

□ Choose a framework that makes sense given your organization’s industry, size, and compliance obligations

Codify which business objectives the DLP program is responsible for enforcing

□ Make these objectives explicit within your program and document them

□ Establish a review process to evaluate your program objectives periodically

□ Security’s goal is business enablement through risk management which means focusing on mitigating high impact sources of risk in revenue impacting areas

□ Communicate your understanding of these objectives to stakeholders and get feedback

Build program policies

Conduct data discovery and leverage data classification to identify and monitor sensitive data

□ Where possible, find technologies that can automate the process of data discovery and data classification

Make sure you understand:

□ **What data do you have?** So that policies can call out specific types of sensitive data by category

□ **Where is the data located?** So you can create policies and procedures that you secure those locations

□ **How should this data be used?** So that policies can specify the appropriate behavior for handling each category of sensitive data

□ **How long should we keep this data?** So that policies can specify explicit retention periods for data

Leverage employees to help codify policies

□ Talk with data owners across different departments to better understand how employees are using data to develop acceptable business uses and retention policies for data

□ Talk with data stewards to help determine how to implement the appropriate configurations for data security and data retention

□ Take this input with results from your data discovery exercise and develop policies that satisfy the requirements of your chosen security or compliance framework

□ Document the individual data owners and stewards in your DLP program

Develop procedures that enable policy enforcement

Adopt controls that allow for proper policy enforcement

□ Controls should provide strong visibility and remediation capabilities while not overburdening admins

□ Document the controls you're leveraging, as well as any unique control configurations

□ Where possible leverage controls that can reliably automate detection and enforcement

□ Create a policy crosswalk or control map

Educate employees who violate policy

□ Use policy violations as a opportunity to educate employees to reduce their chances of repeat offenses

□ Leverage solutions that provide opportunities for just-in-time warnings for employees who are about to violate policy

Create metrics for continuous improvement

□ Start with simple but impactful metrics like the number of incidents per week, month, etc.

□ Advance these metrics into more sophisticated derivative metrics over time, drilling into things like incident severity, cost, or labor impact

□ Get feedback on metrics from stakeholders to engage in continuous improvement

Build processes for breach mitigation

□ Implement a comprehensive breach reporting system that allows stakeholders outside of the security function to report incidents easily

□ Educate stakeholders about reporting breaches and provide strong incentives for doing so

□ Define roles and responsibilities for non-security stakeholders in the event of a breach. This may include legal, compliance, IT, etc

□ Run tabletops or regular simulations so that everyone knows how to respond to breach incidents

□ Create a post-incident review process for continuous improvement

Communicating the value of security to the organization

□ Create regular touchpoints with core stakeholders to solicit feedback and keep them engaged with the DLP program

□ Create a broader form for engaging the entire organization about security-related matters (i.e., newsletters, Q&A sessions, etc.)

□ Highlight the successes of your DLP program and how it's enabling the business when relevant

Learn more about DLP program development

This checklist provided a brief overview of important steps to take in building your DLP program. For a more in-depth look at DLP program best practices, you can read our companion ebook **Demystifying Data Protection: A Blueprint for DLP Program Development**.

Also consider subscribing **to our blog** where we regularly cover DLP best practices and industry developments.

About Cyberhaven

Cyberhaven is the data security company revolutionizing how companies protect their most important information from theft and misuse.

Until now, security products only recognized and protected a limited range of data types because they relied on finding patterns in the content itself. Our data tracing technology analyzes billions of events surrounding every piece of data to better understand and classify it, allowing for protection of a much broader range of sensitive data in any form, anywhere it goes.

To learn more about Cyberhaven, visit

cyberhaven.com