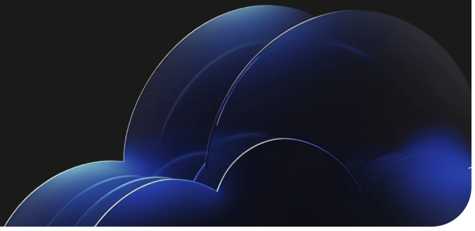
cyberhaven

Demystifying Data Protection:

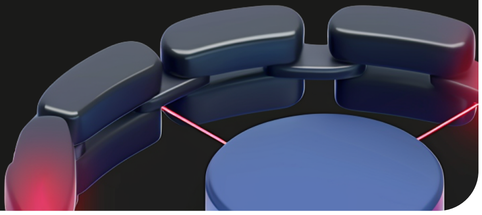
A Blueprint for DLP Program Development

Organizations today face new types of data security risks due to the acceleration of pre-pandemic trends like:

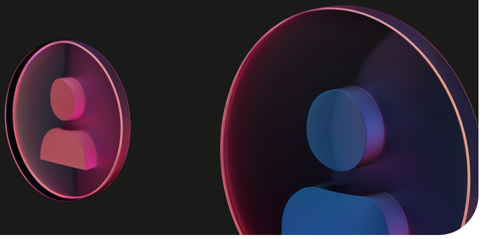
Cloud Adoption



Longer Supply Chains



Hybrid Workforces



Navigating these challenges requires a deliberate approach to data security that includes re-evaluating the tools and processes🔗 that security organizations use to enable the business safely.

Implementing a formal data protection or data loss prevention (DLP) program that provides well-defined policies, stakeholder responsibilities, and clearly scoped security metrics can make it easier to address modern risks while consolidating buy-in for the security function within your organization.

This guide is designed to help security leaders and practitioners, particularly those responsible for working with the broader organization, develop a clear and comprehensive DLP program. We'll talk you through this process and provide examples and quotes from peers so that you can better understand the ins and outs of building your DLP program.

Why you need a DLP program

Enabling data security in a company, organization, or institution is challenging and sometimes thankless. It requires:

Adapting and adjusting security policies as you make tradeoffs between risk and efficiency. Sometimes, this means permitting an "acceptable" level of risk based on the business' risk tolerance.

Building a robust incident response process to address when policies are violated in order to rectify the problem and restore normal business function.

Managing stakeholder expectations in a world where everyone has input on how security should be run.

Communicating these trade-offs to the organization to justify your policies to leadership and employees.

Keeping track of an ever-growing list of threats, so that you can evaluate whether you need to deploy new solutions, policies, and processes to address new challenges.

Balancing budget constraints with the need for advanced security tools and technologies, which often means making tough decisions about where to allocate limited resources.

And much, much more

With a to-do list this long, it's tempting to jump right in by deploying security solutions or creating training sessions to check off boxes to meet compliance requirements and satisfy leadership in the short term. However, experienced security leaders know that putting a formal data security or DLP program in place is crucial for the long-term health and success of the security function.

Why? One of the biggest, well-documented reasons **security initiatives fail** is misalignment with the broader organization's **business objectives** and risk tolerance. The resulting frustration turns would-be stakeholders—like the IT department, C-Suite, and employees outside the security function—from resources into roadblocks who resist security because they don't see the value add, or worse, actively see security as a detriment to enabling the business.

> "As a security leader, it's absolutely critical to align yourself to business objectives. Understand the key mission-critical activities for the business that are driving revenue."
>
> Prabhath Karanth
>
> VP and Global Head of Trust & Security, Navan

Developing a DLP program establishes the business objectives the security function must serve and each stakeholder's role in enabling the broader organization to meet these objectives.

What are the key pieces of a DLP program?

A DLP program aims to document how the security function facilitates business objectives. Your DLP program needs to account for how the policies you create satisfy business goals and how you will enable relevant stakeholders to follow policies with proper standards and procedures. Although the shape your program takes might differ depending on your industry, company size, and regulatory obligations, in the following sections, we'll provide a detailed overview of the considerations you'll want to take into account at every stage of the process.

Some business **process management frameworks**🔗**,** including those for governance risk and compliance or IT security, are designed using "Policy, Standard, Procedure" format where:

01. **Policies** serve as the rules that security organizations enforce that enable safe business operations for their company or organization. An example of a policy might be an acceptable use policy defining business-appropriate use for the company's sensitive data.

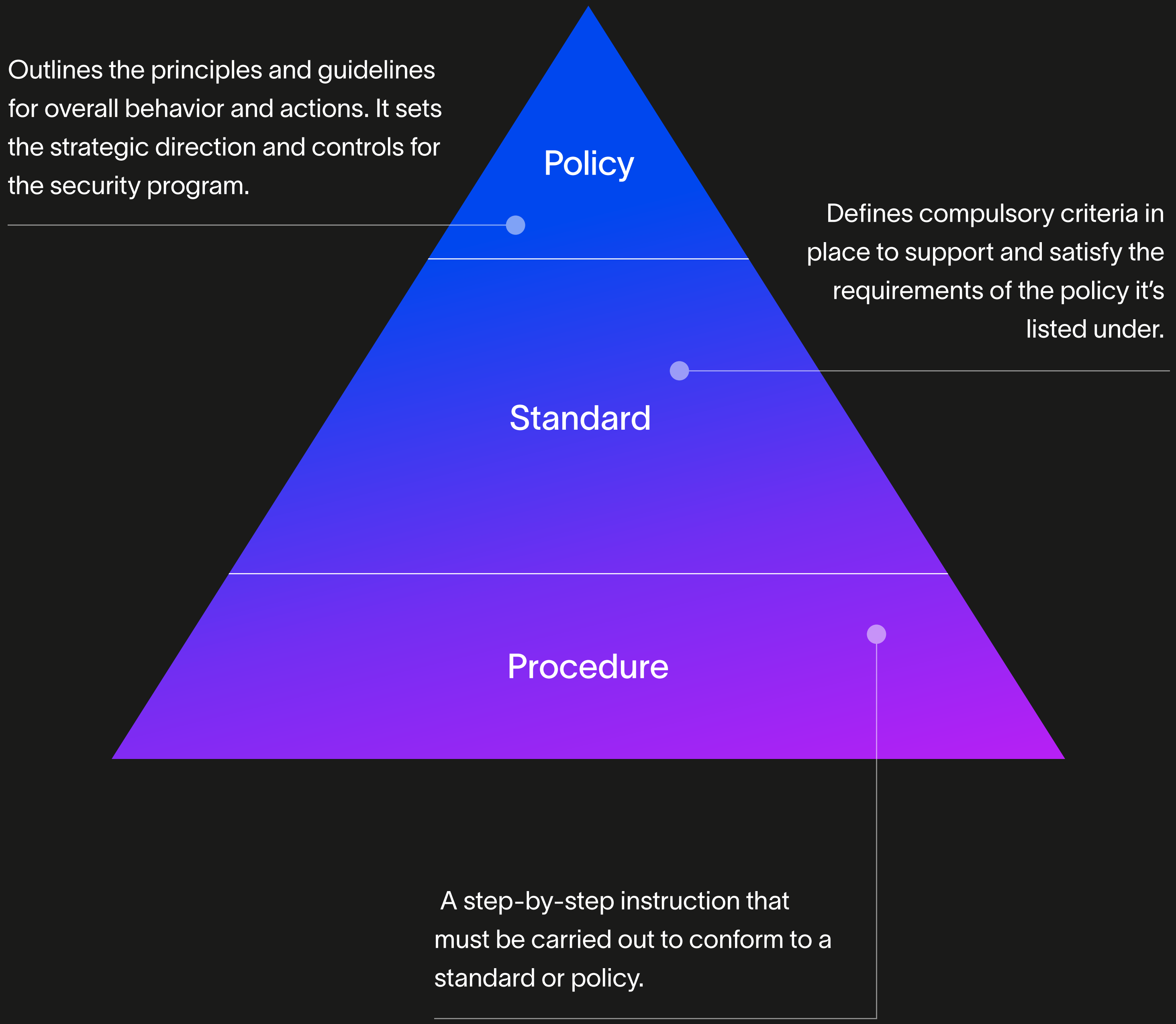
02. **Standards** define the specific criteria that must be addressed to satisfy a policy. Going back to our acceptable use policy example, a standard within this policy might determine the circumstances under which data is business-critical and sensitive. This policy might also have an additional standard specifying where sensitive data is allowed to be stored or moved by an employee and might have exclusions for transferring sensitive data to personal machines.

03. **Procedures** are essential for implementing standards and policies. For instance, in your acceptable use policies, you can outline specific procedures to demonstrate proper security practices. Supplemental documentation for security, risk management, and legal personnel should specify the processes for enforcing and validating these policies, including naming relevant individuals and roles.

Frameworks like those presented in **CISSP** typically depict this relationship as a hierarchical pyramid, with policy at the top. Sometimes, there are **variations in the language** used to describe these concepts; however, the main point is that policies are implicitly designed to roll up to the organization’s objectives, but are supported by standards and procedures. Policies are enforced to enable normal business function, which helps to keep the organization up and running so that it can accomplish its goals.

In this guide we will build from the top and work our way down. Starting with policies that are aligned with business-objectives, using crosswalks and control maps for building standards, then creating procedures that support our policies.

An example of an information governance policy pyramid



Policy

Outlines the principles and guidelines for overall behavior and actions. It sets the strategic direction and controls for the security program.

Standard

Defines compulsory criteria in place to support and satisfy the requirements of the policy it’s listed under.

Procedure

A step-by-step instruction that must be carried out to conform to a standard or policy.

Business objectives are the key driver of DLP program success

Your DLP program will ultimately revolve around the policies you will implement to enable normal operations for the broader organization, as well as the standards and procedures you will implement to ensure that policies are working as intended.

Because of this, it's essential that the first thing you do is outline the business objectives that the security function is expected to enable. Doing so will determine the specific policies and standards that make sense for you to create and implement. In some organizations, objectives may already be documented somewhere and even mapped to existing policies; this might especially be true if you are inheriting a security function or have leadership that works closely with the security organization.

In the absence of this, though, you can take the time to **meet with company leadership and build the partnerships necessary** 🔗 to understand what they're working towards and how they think about business risk. Objectives will, of course, be specific to your company or organization, but below are some examples that illustrate what they could look like:

Safely increasing the organization's ability to drive revenue

A key objective that many security functions will likely want to target is helping drive revenue. The main lever at security's disposal for increasing revenue is lowering risk as the company expands into new markets or acquires new resources. This can be thought of as risk management or, framed more proactively, as business enablement and expanding the organization's capacity to take on new business risks, like corporate acquisitions or moving into new verticals, that can pay off in terms of new revenue sources.

Essentially, the policies, standards, procedures, and controls you put into place can allow the company to take on more challenging responsibilities and external requirements to increase productivity and ultimately revenue. This might take on the form of the following objectives:

- → **Implement** policies, processes, and controls that make it safer for the company to adopt new platforms that increase productivity, like generative AI, without exposing customer data.
- → **Putting in place** processes that demonstratively satisfy specific requirements for partners and customers to allow the organization to increase revenue by working with more stakeholders without increasing data exposure risk.
- → **Creating** offboarding processes that enable the organization to maintain the confidentiality and integrity of sensitive data, even during times of high employee turnover.

Satisfying regulatory requirements

For organizations that must comply with specific regulatory frameworks, the security function explicitly serves a core business objective in enabling the company to meet its legal obligations while preventing the loss of revenue from fines. Regulations sometimes detail functionality that the organization is expected to be able to carry out. This somewhat dictates what your policies, which will solve for compliance, should look like.

For example, complying with the GDPR explicitly requires the ability to conduct a Data Subject Access Request (DSAR), which mandates that an organization must identify all the data it has collected and processed about a specific individual whenever a request is submitted. Conducting DSARs means that the organization must have the infrastructure in place to accept customer requests, discover customer data within systems, and produce the results of this process.

As a second example, the HIPAA security rule lists over 34 implementation specifications for healthcare organizations, which are standards that the organization's information security program needs to have in place to satisfy HIPAA compliance requirements. If you're working on building a DLP program for a healthcare organization, your policies need to touch on the ways you're addressing these implementation specifications.

Do's for creating business-aligned objectives:

→ **Work closely with Legal, Risk, Compliance, and Executive stakeholders**

Regularly engage with these stakeholders to understand the legal, financial, and operational aspects that shape business objectives.

→ **Conduct thorough business process reviews**

Understand how different business units operate and how data flows within these departments. This insight is crucial for setting DLP objectives that are relevant and supportive of these operations.

→ **Establish clear communication channels**

Ensure there are regular and clear communication channels with all stakeholders for updates, feedback, and decision-making. These can be anything from chat groups to recurring business meetings.

→ **Document and map business objectives**

Clearly document and map the organization's objectives against requirements. This helps in creating a DLP strategy that directly supports these objectives.

Don’ts for creating business-aligned objectives:

→ Avoid rushing into policy creation

While it’s important to move forward with policy development, avoid rushing into it without a sufficient understanding of business needs and risk landscape.

→ But also steer clear of analysis paralysis

Balance thorough analysis with the need for action. Avoid getting so caught up in data and consultations that decision-making and policy development are significantly delayed.

→ Don’t work in silos or neglect stakeholder feedback.

Avoid creating DLP objectives in a vacuum. Input from various departments is crucial to ensure the objectives are comprehensive and aligned with business needs. Consider their insights and concerns before setting goals.

→ Don’t overlook evolving business needs

Business objectives can change over time. Ensure that the DLP objectives are flexible enough to adapt to these changes.

Building DLP policies from business-aligned objectives

As stated in the last section, policies are core to carrying out the objectives of your DLP program. Policies will inform the processes and tools you implement to achieve your business-aligned objectives. To understand the process of translating objectives into policies, it first makes sense to think about the questions you'll need to answer when building your data protection policies. **Broadly, you'll want to know the following:**

01. **What data do we have?** Your DLP policies must explicitly call out business-critical or sensitive data by category. Business-critical data is data whose exposure poses a risk to the organization.

02. **Where is this data located?** You should have an understanding of where this data is located within your environments.

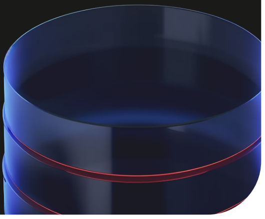
03. **How should we use this data?** Answering this question means defining the boundaries of acceptable use for business-critical data, including what constitutes business-relevant activities, how specific categories of data are allowed to be shared, and where they should be stored.

04. **How long should we keep this data?** Retention is sometimes an overlooked aspect of data security. Keeping sensitive data around longer than necessary can pose some amount of risk. However, this ought to be balanced with business needs.

Answering these questions gives you a sense of conditions at the operational level of your business, which is essential when evaluating how to quantify risk. Additionally, this will help you define and enforce the behaviors enabling your organization to lower risk and continue normal operations without impediment.

To better understand the nature, location, and use of business-critical data within your organization, you'll need to conduct activities like data discovery, data classification or tagging, and speaking to employees who function as admins within the applications and services used by your organization.

> "Preventing data loss is the end goal which you enable through policies and enforcement. Data classification is what makes this possible. It's so important that you'll need to backtrack if you haven't done it, which is a lot of work."
>
> Kheun Chan
>
> Principal Security Architect, Iron Mountain

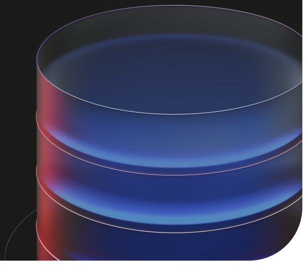


Conducting data discovery and classification at scale with data lineage

Data discovery and classification can be challenging, especially when tackling it at scale. This isn't a process you want to rush, however, as the point of this exercise is to get an accurate sense of the type of data you have within your environments so that you can create a formal classification process and design informed policies that enable you to accurately address risk within your organization.

Security practitioners are increasingly turning to automated tools that enable data discovery and automatic and accurate data classification. Next-generation data protection platforms like Cyberhaven can classify data in motion or identify whenever a user takes an action against a piece of data, like cutting it, copying it, or similar actions. This capability, known as **data lineage**, allows for more accurate findings. It enables security administrators to capture details like where data originated from, the users who accessed it, and more. This metadata exists alongside more traditional data classification data captured with regex and other rules.

> “We find it extremely refreshing how Cyberhaven doesn’t require data classification until the data starts moving. Seeing that was just eye-opening. I don’t have to do this massive amount of homework before I can understand what’s in my environment.”
>
> Michael Traski
>
> Director of Information Technology, IVP



Cyberhaven users, like Michael Traski at the industry-leading venture capital firm IVP, have deployed Cyberhaven to conduct data classification. Before using Cyberhaven to enforce policies, IVP monitored their endpoints and applications to better understand what data their users created and modified as part of their role and determine where this data was egressing. This proved to be immensely valuable in helping orient IVP’s program and identify opportunities around what behaviors to coach and educate end-users about to minimize future incidents.

Throughout this process, Michael spoke to employees about their work to better inform his understanding of the patterns he saw when first monitoring environments with Cyberhaven. By understanding people’s roles and responsibilities, Michael could begin to think about how to build policies in a way that wouldn’t impact user productivity.

Turning employees into stakeholders to develop retention policies

Tools like Cyberhaven can help you learn about the types of sensitive data within your organization, where it is, and how users share it. However, to understand retention, you will need to speak with users directly. Doing so will give you a sense of how users intend to access data in the future.

Talking to department leadership first might make sense to determine whether policies are already in place. For example, the marketing team might have a policy or practice that has them retain customer PII indefinitely, whereas HR might remove the PII of former employees after two years.

When speaking to employees about their recordkeeping and retention practices, you should delineate between employees who merely access the data and those with admin or advanced permissions in the environments where this data is stored. You can think of the former as "data owners" and the latter as "data stewards." **Briefly:**

→ **Data owners** 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.

→ **Data stewards** are employees who are application owners and are the ones who will ultimately set the retention policy for data within the environments where it's being stored or shared because they have admin access in these systems. Conversely, they may have the greatest need for retaining data for long periods. For example, this might be a sales operations person within the sales department or an HR leader who recently inherited access to the organization's main HR platform after a downsizing.

With your DLP plan, you should codify who data owners and stewards are for your organization's different types of business-critical data. You should also work closely with data stewards to regularly review retention policies and change them as needed.

Mapping learnings from data classification and stakeholder discussions to security frameworks to design standards

Once you've conducted data classification and spoken with employees to better understand data flow and retention throughout your organization, you'll be in a better position to begin building security policies mapped to business objectives. This process can be more art than science. One of the most common starting points for teams engaged in this exercise is to leverage existing security or compliance frameworks. This process can be fairly straightforward for organizations held to regulatory compliance requirements or industry standards like SOC 2 or PCI DSS. Many of these frameworks provide explicit controls and functions that your DLP program is responsible for carrying out in order to protect data.

In the previous section, we provided examples of GDPR and HIPAA, but this insight also applies to industry-driven compliance frameworks. For example, for payment vendors, the PCI DSS requires that you monitor out-of-scope systems (systems where customer card data shouldn't be) to ensure that such systems remain clear of Primary Account Number information or PAN.

Organizations that aren't explicitly subject to requirements like these are free to adopt general-purpose security frameworks like ISO 27001, DSMM **(Data Security Maturity Model)**🔗, and others that provide excellent scaffolding for building policies.

Two small steps you can take when leveraging security framework includes:

→ **Identifying compliance or security frameworks that suit your program.** Selecting the proper security framework for DLP policy development involves thoroughly understanding your organization's industry, regulatory requirements, risk profile, and operational goals. While no framework is terrible, some frameworks have a specialty or focus that they're optimal for. For example HITRUST, an industry-standard framework, is ideal for supplementing the information security programs of enterprise healthcare organizations. Alternatively, something like NIST CSF is designed to be small and flexible enough for organizations of any industry or size, and there are more readily available resources on adopting NIST CSF as it's an open standard. Keep these considerations in mind when deciding between frameworks.

→ **Conducting exercises like policy crosswalking or control mapping to connect your policies and objectives to enforceable security standards.** Security teams often perform exercises like building a **policy crosswalk**🔗 or **control map**🔗 to correlate their internal policies to the frameworks and compliance requirements they're using to inform their DLP program. Basically, doing a policy crosswalk or control map allows you to correlate your internal activities, including controls and policies, to the requirements they satisfy.

Beyond this, organizations like the SANS Institute provide **policy templates**🔗 for a wide range of information security requirements like encryption and employee data use. You could choose to use these as a starting point to map to a compliance framework.

Do's for building DLP policies from business-aligned objectives:

→ Automate data discovery and classification wherever possible

Before establishing policies, it's crucial to comprehend the data layout in your environments. While taking the necessary time, avoid prolonged manual tasks by utilizing automated tools that leverage data lineage for a faster process.

→ Speak with employees throughout the data discovery and classification process, even when using automated tools

When classifying data, understand the daily tasks of employees in departments handling critical data. Communicate with them to grasp their responsibilities, ensuring seamless implementation of processes and tools without disruption

→ Build relationships with data owners and data stewards

Work closely with data owners and stewards to understand what data each department manages and how long this data should be retained. Continue to keep in touch with them so that you can better understand any changes in use or retention of data.

→ Leverage security frameworks to make policy planning easier

Utilize security or compliance frameworks and conduct policy crosswalking or control mapping to align your internal policies with these frameworks.

→ Consider framework specialties and focus

When selecting a framework, consider the specialty or focus of the framework and how it aligns with your industry and organizational size. Also, choose frameworks based on their flexibility towards future business changes and growth.

Don’ts for building DLP policies from business-aligned objectives:

→ Don’t rush the data discovery and classification process

Avoid hurrying through the data discovery and classification process. Take the time to accurately understand the data landscape within your organization.

→ Don’t overlook employee input in policy formation

Do not ignore the insights from employees who interact with data daily. Their input is vital in shaping practical and effective policies. Communicate with stakeholders throughout the process to understand the data and procedures currently in place.

→ Don’t choose a framework solely based on popularity

Avoid selecting a security framework strictly because it is popular or widely used. Choose one that specifically aligns with your organization’s needs and objectives.

→ Don’t neglect changing business needs

Do not set retention policies in stone. Regularly revisit and adjust them to meet evolving business needs and regulatory changes.

Crafting processes for your DLP success

Once policies have been codified, security teams will need to implement procedures that allow policies to be managed and maintained. **These include:**

- **Building out procedures for policy enforcement.** You'll need to put into place the processes that identify the types of activities that constitute violations of your policies, then decide the controls you'll use to carry out enforcement and what actions will be taken to prevent or rectify violations.

- **Creating and evaluating metrics to judge and iterate on program performance.** Metrics need to be implemented to assess if your DLP program and policies are causing risk to trend downward for your organization.

- **Conducting audits and reviews of your program performance with internal and external stakeholders.** You'll need to decide on a regular cadence for audits and agree on a process for conducting audits and a method to share this information with key stakeholders.

- **Create a runbook for data exposure incidents.** In the event that an unmitigated incident occurs, you'll need to have procedures in place to address the incident and help the organization resume normal function.

- **Additionally, build out a communications function for your security organization.** Enhance process visibility, involve stakeholders for feedback in your DLP program.

Enabling policy enforcement at scale

Policy enforcement is where the rubber will meet the road for your DLP program. Enforcement will be how you identify and mitigate incidents before they become bigger risks. The good news is that building the enforcement mechanism of your DLP program is an iterative process that will only improve as you get more feedback from internal audits of incident reports and stakeholders providing feedback on metrics and satisfaction.

As part of your control mapping or policy crosswalk exercise, you should have identified security controls that make sense for identifying incidents and enforcing your policies. Like with data discovery and classification, here you should leverage tooling that can intelligently automate incident reporting and automate remediation for any routine incidents. This typically means avoiding legacy solutions that handle DLP, Insider Risk Management (IRM), and Security Information and Event Management (SIEM) as distinct from one another and require extensive setup to integrate with one another.

Essentially, all security teams that leverage Cyberhaven to conduct their data discovery and classification exercise to better understand their risk end up building their DLP program around the platform as a reporting and remediation tool. This is because of how well Cyberhaven understands the context surrounding data in your environments, which is critical for granularly addressing risk.

> “What do you need a SIEM tool for? They are a first-generation way of approaching incident detection. Our goal has always been to get better insight. I don’t want to just see what’s being stopped. I want to know where it came from, who did it, and why. Now, I get to see a whole picture of everything that’s going on, regardless of whatever rules, policies, or datasets that I’ve set up.
>
> Chris Payne
>
> VP of Information Security, VaxCare

Effective enforcement planning combines the insights gained from data discovery and classification with the strategic configuration of tools to prevent improper data egress. This requires meticulous documentation to ensure admins understand the specific application policies and settings required to identify risk, push alerts, and automatically remediate security incidents. Once tools are operational, there should be regular security reviews of incidents to continuously evaluate risk.

Another aspect of enforcement that might sometimes be overlooked is the human aspect. While controls and tooling take care of the work of identifying incidents and rectifying the actions that triggered them, consider having procedures in place to educate or address users who cause incidents.

For example, many Cyberhaven users leverage a feature that allows admins to send just-in-time notifications to users who are about to violate a policy, alerting well-meaning employees about the risk of their actions and even giving them the option to provide a justification to override the block if they have a genuine business justification for carrying out their action.

> “What used to happen with our prior DLP tools is employees would try to send an email that would get blocked and get no feedback. So they’d try to send it again and again. It’s important to have tools in place that can explain to users what policies they’re violating and what other options they have to accomplish their goal. Having these additional presentation tools has been very helpful in making employees feel less frustrated.”
>
> Chris Payne
>
> VP of Information Security, VaxCare

In tandem with this, other Cyberhaven users, like the team at IVP, use the incident data from Cyberhaven to identify opportunities for coaching for individual users who’ve repeatedly violated policy to understand where the disconnect may lie. You may implement a procedure like a “three strikes” rule to do a manual or in-person follow-up with users who have violated policy three times within a given period (like over a quarter, for example). This action can be codified as part of the communications function you build to engage stakeholders to better accomplish objectives.

Do’s for building DLP enforcement capacity

→ Identify and leverage controls that can consolidate and automate parts of enforcement.

Choose controls that offer automation and consolidation for various aspects of enforcement, such as alerting, reporting, and remediation.

→ Configure your controls based on your policies

Tailor your security controls to align with your established DLP policies and regularly update these configurations to reflect any changes in policies or the risk landscape.

→ Document control configurations

Maintain clear documentation of all control settings and configurations. This is crucial for ensuring consistency, facilitating audits, and troubleshooting. This documentation should be accessible to all relevant personnel and updated whenever configurations change.

Don’ts for building DLP enforcement capacity

→ Don’t forget the human touch required for enforcement

Enforcement and education go hand in hand. Address incidents involving employees with a focus on education and understanding rather than purely punitive measures. Regularly engage with employees who have repeatedly violated policies to understand the root cause and provide targeted coaching or training.

Improving enforcement over time with metrics and audits

As mentioned in the section above, policy enforcement is an iterative process, with the efficiency of the enforcement improving over time. Part of how you drive those efficiency gains will come down to the metrics and feedback you gather to inform areas of improvement for your program. Monitoring incidents, producing metrics, reviewing feedback, and applying the feedback to your program can be viewed as a **continuous improvement process**. Such processes are standard in domains where quality assurance is critical for stakeholders—like customer service or manufacturing—and are becoming common **in IT and security**. With this being the case, it's highly likely that the metrics you start out reporting on may be replaced by different metrics as your program matures, you get more feedback, and your objectives change. Don't let this give you pause; embrace continuous improvement by approaching the process of identifying and reporting on metrics as an experiment.

Start with low-hanging fruit to gather metrics and report quickly

The question of what data protection metrics the security organization should focus on could fill an entire book, but you can start by focusing on something simple. To illustrate this, we'll return to IVP's security program. One of the first metrics IVP's security team started evaluating after deploying Cyberhaven was incidents per week to establish a baseline of how frequently inappropriate handling of data was occurring. The team initially tracked this number weekly to be able to attribute changes to specific actions they took. For example, when they first began enforcing the data security policy with Cyberhaven, they made a company-wide announcement about the platform and the data security rules in place. There were no incidents in the first few weeks, which they could attribute to their announcement remaining top of mind for employees.

However, eventually, the team began seeing incidents increase. They conducted interventions with specific users who violated the policy to see how that impacted the total number of incidents, which yielded positive results very quickly. They tracked a week-over-week reduction in incidents as a result of their efforts.

This is far from the only metric used within IVP's program, but it demonstrates a great approach to standing up metrics and reporting if you're unsure where to begin. Tackling low-hanging fruit, like the frequency or occurrence of incidents, can be a useful launchpad for starting quickly. Once you've done that, you can create derivative metrics that further refine the scope of what you're tracking before expanding the number of areas you evaluate across your program.

Using the number of incidents per week as an example, some derivative metrics we can create include:

- **Change in incidents over time.** This is what IVP did when they tracked the change in incidents week-over-week. They went from simply observing the number of incidents that took place in a single week to following this measure over time. This gives a trendline that allows you to understand the direction in which outcomes for your security program are being influenced, as we illustrated above.

- **Severity of incidents.** Once you have metrics on the incidents occurring in your environments, you can start drilling down into how risky incidents are. You'll have to categorize incidents or risks based on your business needs and objectives. Document these as part of your processes and procedures so everyone evaluating this metric is on the same page.

- **Impact on labor hours.** If you have a significant reduction in the number of incidents that analysts are triaging, this effectively results in a decrease in labor hours, freeing up time within the security function to work on more critical tasks. This can be quantified and illustrated to stakeholders as a benefit.

- **Impact on cost.** Similar to the above metric, a reduction in incidents can be correlated with a cost reduction. For example, you can put a dollar amount on the saved labor hours resulting from reduced incidents. Or you can devise a metric to put a price on a security incident by attributing a cost per record of specific data types. Some practitioners use the costs found for data on the **dark web** or costs used in reports like IBM's annual **Cost of a Data Breach Report**. Over time, you might be able to tailor these costs to be more specific to your industry or organization, but using resources like these to price risk can be an acceptable starting point.

Once you start collecting metrics, you can begin reporting them to key stakeholders for external feedback. You should also internally review these metrics to ensure your program moves in the right direction. Review sessions with stakeholders should occur regularly and provide space for the security organization to demonstrate how metrics map to business objectives and solicit feedback from the broader company based on timely and relevant developments within the business.

Do's for for standing up metrics and reporting in your security organization

→ Start with simple but impactful metrics

To establish a baseline, identify and track straightforward metrics, such as the number of incidents per week. This approach allows for the quick gathering of actionable data. These can eventually be evolved into more nuanced derivative metrics before you expand into developing metrics for other areas of your security function.

→ Get feedback from stakeholders regularly and often

Hold regular sessions with stakeholders to present how the metrics align with business objectives and to gather their input. This ensures the security program remains relevant and aligned with the broader organizational goals.

→ Conduct internal reviews of security metrics, too

Conduct frequent internal reviews of security metrics to assess the direction of your security program.

Don’ts for for standing up metrics and reporting in your security organization

→ Don’t forget the importance of continuous improvement

Avoid sticking rigidly to initial metrics. Be prepared to evolve and replace metrics as your program matures and as you receive more feedback and insights. Embrace continuous improvement and view metrics as an evolving tool to refine and enhance your security program.

Build your incident runbook to mitigate breaches

Sometimes, you might discover incidents outside of your enforcement and review process. Perhaps an employee or some other stakeholder alerts you to an incident. Realistically, it’s not security’s job to guarantee that the organization **will never be breached** but to put processes in place that minimize the severity of incidents that do occur. The point of having a DLP program and documenting your processes is to codify this so that the entire organization understands how your program will address risk when breaches happen.

One of the most important pieces required to execute this is having the capacity to intake detailed submissions or reports of incidents from stakeholders like employees. If the security team is the only part of the organization looking for incidents, some will likely be missed. Doing this well means educating stakeholders about the signs of a breach, as well as the factors that go into determining the severity of a breach.

Additionally, create a security runbook to address breaches, defining breach criteria based on industry, compliance, and regulatory obligations. Incorporate post-incident requirements outlined by legal frameworks such as HIPAA and CCPA, or non-regulatory frameworks like NIST CSF, which can inform the actions required to resolve incidents and restore normal operations.

Once you understand the responsibilities that need to be carried out after a breach, you should write them down in your runbook and assign them to relevant individuals within your organization. For example, if there are reporting requirements for incidents based on your industry, you should loop in individuals from the legal or risk teams to play a role here. In general, you’ll want to identify individuals close to business operations who can assist with business continuity should a breach disrupt operations.

Do’s for building a runbook for breaches

→ Implement a comprehensive breach reporting system

Develop a system that allows non-security stakeholders to report incidents easily. This could be a dedicated hotline, an online reporting form, or an email address. The key is to make it accessible and user-friendly.

→ Educate stakeholders on reporting incidents

Provide clear guidance to all employees and stakeholders on recognizing and reporting security incidents. Regular training sessions and communication materials can raise awareness about this reporting system.

→ Leverage regulatory compliance and security framework requirements to build your runbook

Customize your runbook to align with your industry’s specific compliance and regulatory requirements and your organization's unique risks. Make sure to consult the same security and regulatory frameworks you used to build your policies to derive guidelines for resolving incidents.

→ Assign clear responsibilities to specific individuals/roles

Identify and involve relevant stakeholders from legal, risk, IT, and business operations to ensure a comprehensive response to breaches. Also, define and assign responsibilities for breach response to specific individuals or roles within your organization. This ensures accountability and efficiency in responding to incidents.

Don’ts for building a runbook for breaches

→ Avoid limiting runbook accessibility

Ensure that the runbook is readily available to all stakeholders across the organization. Avoid keeping it confined within the security team.

→ Don’t ignore regular training or tabletops around runbook processes

Avoid assuming that stakeholders will know how to use the runbook without proper training. Conduct regular training sessions to familiarize them with the procedures and their roles in the event of a breach.

→ Don’t forget to update the runbook processes in a timely manner

Keep the runbook updated with the latest procedures and ensure it’s easily accessible, possibly through an intranet or a central documentation repository.

→ Don’t neglect post-incident review processes

Use post-incident reviews to identify lessons learned and areas for improvement in the runbook and solicit feedback from stakeholders to continuously improve the runbook.

Creating a communications function that meaningfully engages stakeholders

We've touched on communication throughout this eBook, but it's worth building an explicit communications function led by someone on your team if you have the capacity to do so. This doesn't have to be a substantial investment; you just want to ensure regular communications with your stakeholders. For example, the security teams at IVP and Vaxcare have a monthly newsletter containing updates and tips that help employees keep security in mind.

Beyond that, it could make sense for your program to ensure, as part of your regular communications, that you have an open window policy to invite stakeholders to provide feedback on your program, even outside of review sessions.

Finally, wherever possible, you should highlight security successes in your communications to the broader organization and the stakeholders' role in contributing to those successes. Because your DLP program will be connected to business objectives, over time, you'll be able to show in detail how security impacts the bottom line and how your stakeholders are helping to make this possible.

Putting this guide into action

This guide provided an overview of important steps to take in building your DLP program. To help make this content actionable, we've summarized everything into our complimentary **Data Protection Checklist**🔗. Download our checklist to help guide you through the most important steps of this guide.

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

cyberhaven

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