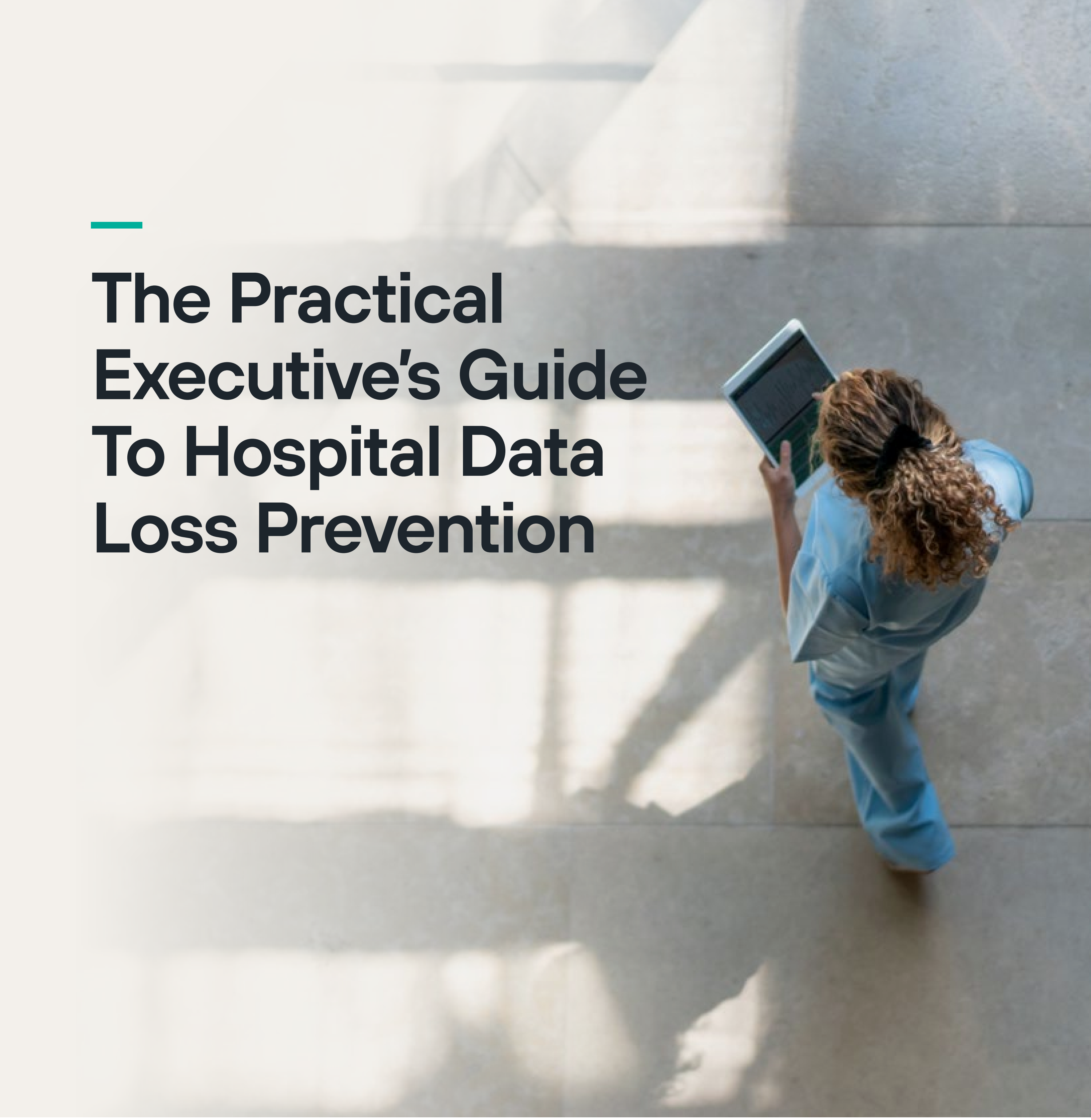
The Practical Executive's Guide To Hospital Data Loss Prevention



Forcepoint

Whitepaper

forcepoint.com

Table of Contents

Introduction

When hospital data breaches and exfiltrations occur, lives may be put at risk. Just one data breach takes a hospital an average of 329 days to identify, and 93 more days to remediate.[1] In the meantime, research shows hospitals experience an increase in death rates, particularly among heart patients.[2]

In addition to stopping breaches, hospitals are tasked with securing patient privacy. This is more than a HIPAA compliance requirement. Patients are becoming more savvy about protecting their privacy rights, especially as the global pandemic has spurred discussions around solidarity-based healthcare, which focuses attention on public health.

Because of rising data security awareness and higher safety standards, hospitals are attracted to Data Loss Prevention (DLP) solutions, which help with data breach protection, fair patient data use, and transparent reporting. Another benefit of DLP solutions: they provide hospital staff with safe access to patient and medical data from remote endpoints. But with the revenue pressures introduced by COVID-19, hospitals must ensure every cybersecurity investment provides their organization with the precise protection they need.

When evaluating DLP options, it’s important to realize that not all solutions are created equal. It’s not the technology alone that ultimately determines your DLP success. Rather, your results are determined by how well a solution’s capabilities support your DLP goals and execution strategy (i.e., traditional or risk-adaptive, as described in the following section).

This guide outlines nine steps to your hospital’s DLP success. You’ll also find guidelines and suggestions to help you:

→ Assess DLP vendors

→ Wisely allocate your security resources

→ Create practical and measurable DLP controls

→ Avoid common DLP pitfalls.

DLP Security Controls: Standard and Advanced

DLP controls will help your hospital to reduce security risks associated with sensitive personally identifiable information (PII), protected health information (PHI), and medical data by enforcing policies and security best practices.

Now let’s take a look at the functionality that allows DLP solutions to do this.

1. They provide the ability to identify data.

→ Data-in-Motion (traveling across the network)

→ Data-in-Use (being used at the endpoint)

→ Data-at-Rest (sitting idle in storage)

→ Data-in-the-Cloud (in use, in motion, at rest)

2. They identify data as described or registered.

→ Described: Out-of-box classifiers and policy templates help identify types of data. This is helpful when looking for content such as PII.

→ Registered: Data is registered with the system to create a “fingerprint,” which allows full or partial matching of specific information such as intellectual property (IP).

3. They take a risk-adaptive approach to DLP (advanced capability)

→ Risk-adaptive DLP sets advanced data loss prevention solutions apart from the other DLP tool sets. Derived from Gartner’s continuous adaptive risk and trust assessments (CARTA) approach, risk-adaptive DLP adds flexibility and proactive response to DLP. It autonomously adjusts and enforces DLP policy based on the risk an individual poses to an organization at any given point in time.

Identifying data in various states (#1 and #2) are standard capabilities for all DLP controls. However, a more advanced DLP solution will also be equipped with risk-adaptive capabilities (#3).

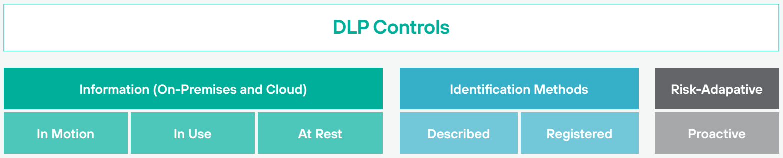
To illustrate how the first two common capabilities work, a DLP control is told:

→ What to look for (e.g., credit card numbers)

→ The method for identifying the information (described/registered)

→ Where to look for it (e.g., network, endpoint, storage, cloud)

What happens after a DLP control identifies the information depends on a) the risk tolerance of the data owner, b) the response options available when data loss is detected, and c) whether the solution is risk-adaptive.



[1] IBM Security, 2020 Cost of Data Breach Study

[2] Health Services Research, “Data breach remediation efforts and their implications for hospital quality,” November 2019

From Vision to Implementation

Although all DLP controls provide similar capabilities, it's important to understand that not all vendors have the same vision for how DLP helps to address the problem of data loss. Therefore, to ensure your hospital's implementation will be effective, you must first understand each vendor's DLP vision and methodology.

By asking a vendor, "What's your DLP vision and methodology?" you are really asking, "How do you see this tool solving the problem of data loss?" This is an important, yet rarely asked, question. The answer allows you to understand a vendor's vision, which in turn enables you to identify its tool's unique capabilities and the direction the product roadmap is likely to head.

A vendor's methodology also heavily influences its execution or implementation strategy. For example, if one vendor's methodology starts by assessing data-at-rest, and another's starts by assessing data-in-motion using risk-adaptive controls, then their execution strategies differ greatly. How a vendor executes DLP controls matters because it impacts both your hospital's total cost of ownership (TCO) and expected time-to value, which are crucial for making the right purchase decision and for properly setting stakeholder expectations.

An important note: you should avoid applying one vendor's methodology to another's technology. The methodology defines and drives a vendor's technology roadmap, so by mixing the two aspects, you risk investing in a technology that won't meet your long-term needs.

Measurable and Practical DLP

If you've attended a conference or read about DLP best practices, you may have com across sweeping generalizations like, "Don't boil the ocean." Aside from warning DLP practitioners against taking on too much at once, how useful is this "best practice," really? It doesn't help your hospital figure out what to do and when to do it.

Unfortunately, many published DLP best practices aren't always practical for every hospital. Lack of resources, financial or otherwise, and other organizational issues often leave "best practices" unfollowed. The best DLP guidelines are practical. They factor in the cost, benefits, and effort of following them, and can be measured to determine whether you and your hospital can or should adopt them.

To ensure your DLP controls are both measurable and practical, you'll need two key pieces of information:

1. **The risk model for data loss:** When you apply this formula, you'll be able to measure the effectiveness of your DLP controls.

2. **The 80/20 rule:** Use this principle to focus your attention and resources on areas that are most likely to experience a high impact data breach.

Now let's look at the data loss risk model and the 80/20 rule in more detail.

The Risk Formula for Data Loss

The basic risk formula that most of us are familiar with is:

Risk = Impact x Likelihood
The challenge with most risk models is determining the likelihood, or probability, that a threat will happen. This probability is crucial for determining whether to spend money on a threat-prevention solution, or to forego such an investment and accept the risk.

The difference with the risk formula for data loss is that it doesn't deal with the unknown. Instead, it acknowledges data loss as inevitable and usually unintentional. Most importantly, the data loss risk formula allows risk to be measured and mitigated to your hospital's comfort level.

Therefore, the metric used for tracking reduction in data risk and ROI of DLP controls is the rate of occurrence (RO).

Risk = Impact x Rate of Occurrence (RO)
The RO indicates how often, over a set period of time, data is used or transmitted in a way that puts it at risk for loss, theft, or compromise. To calculate the amount of risk reduction, you should measure the RO before and after you execute DLP controls.

For example, if your hospital starts with an RO of 100 security incidents in a two-week period, and is able to reduce that amount to 50 incidents in two weeks following DLP control implementation, then you have reduced the likelihood of a data-loss incident (data breach) by 50%.

If one of the DLP solutions you are comparing has risk-adaptive technology, it is likely to show a smaller RO. This is because risk-adaptive DLP is far more accurate at identifying risky user interactions with data, so it generates fewer false positives and a lower overall RO. This presents an advantage over traditional DLP solutions. However, it also makes comparing the reduction in risk a bit more tricky.

We recommend that you review and verify each incident produced by the non-risk adaptive technology to ensure it is not a false positive. Just because the identified data matches the DLP rule, it does not necessarily mean the data violates policy. You should also inspect the intent and context around the data loss incident to ensure the incident is, in fact, a true positive.

The 80/20 Rule of Hospital DLP

In addition to identifying RO, it's important to identify where your hospital is most likely to experience a high-impact data breach. To do this, research the latest healthcare breach trends and then use the 80/20 rule to determine where to focus your DLP efforts.

Since the onset of the pandemic, more of your clinicians are working outside hospital walls—and more data is circulating outside your network. How much data are we talking about? Consider these statistics: During the COVID-19 lockdown, organizations saw an 80% increase in the movement of data outside their networks, including a 123% increase in the volume of data moving to USB drives and a large spike in data uploaded to cloud storage services.[3] Meanwhile, the FBI reports that online scam complaints have increased by 400% since the onset of the pandemic.[4]

In this new normal , your data loss protection must extend to secure remote staff and data movement through web, email, cloud, and removable media.

This is where a risk-adaptive DLP solution can provide your hospital with an advantage. Traditional DLP solutions often struggle to identify items, such as broken business processes or irregular activity, both of which can lead to significant data loss. However, risk-adaptive DLP understands the behavior of individual users and compares them to their peer groups; this behavioral context equips the solution to quickly and autonomously tighten DLP controls when activity is not in line with the end user's job function. Armed with this proactive approach, your hospital can reduce risk for accidental data loss and exposure.

[3] "FBI sees spike in cyber crime reports during the coronavirus pandemic," *The Hill*, April 2020
[4] Interpol, 2020

The Forcepoint DLP Vision

Considering data breach trends and applying the data loss risk formula are important first steps towards developing a data loss prevention strategy for your hospital. The most effective DLP programs go farther; they concentrate on understanding user intent to prevent data loss before it occurs. We call this "human-centric cybersecurity." To execute this approach, your team should focus on providing the best time-to-value for demonstrating a measurable reduction of risk.

Time-to-Value: Pitfalls and Pointers

Time-to-value is the difference in time between implementing DLP controls and seeing measurable results in risk reduction. For example, if most of your hospital's data breaches occur from insiders (accidental or compromised), you'll get the best time-to-value with DLP that is focused on data-in-motion and data-at-rest using risk-adaptive technology in the background.

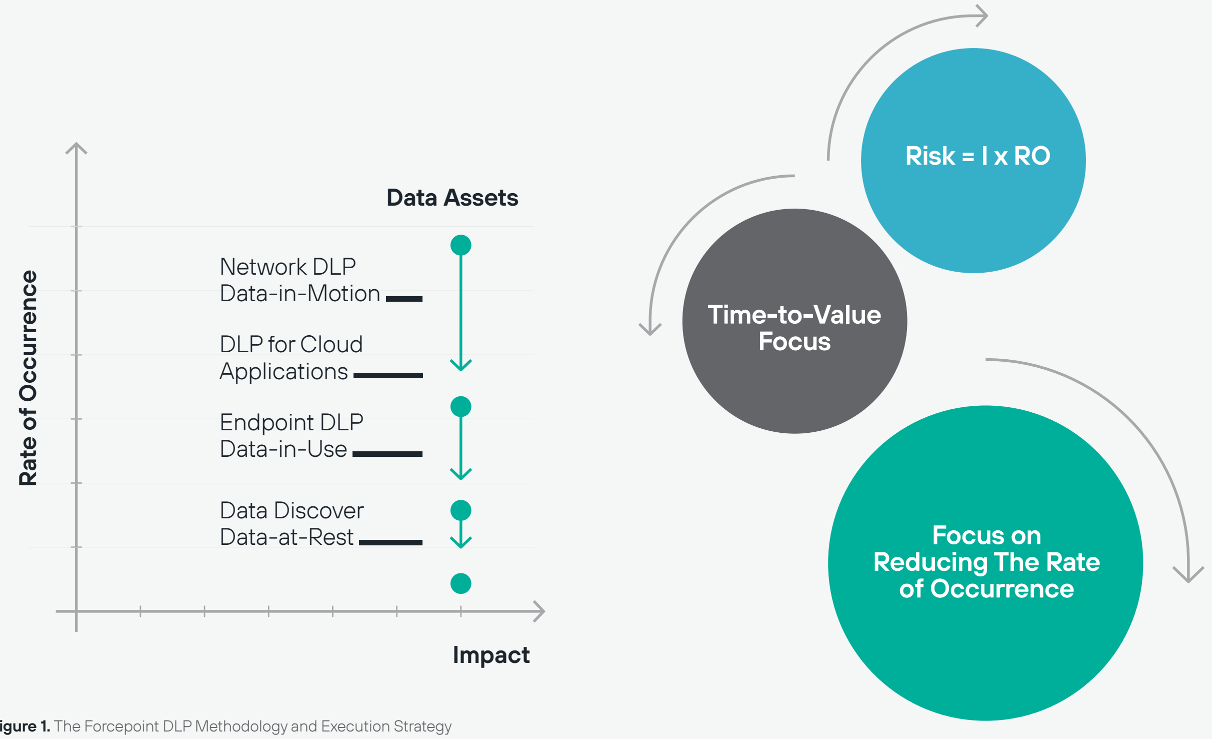


Figure 1. The Forcepoint DLP Methodology and Execution Strategy

If you've been told by other vendors or thought leaders to focus first your DLP controls on data-at-rest, you might be scratching your head. You might have heard, "If you don't know what you have and where it is located, then you can't expect to protect it." But this is not true; in fact, DLP controls are designed to provide this protection. Either the other vendors and experts don't understand how to properly assess and address risk, or they are simply repeating what others say because it seems to be working for them.

Focusing on data-at-rest at the outset is problematic because it focuses on implied risk, not actual risk, and therefore it cannot be measured in the context of risk reduction.

Implied risk requires other conditions to be met before a negative consequence can happen. In the context of data loss, those conditions are:

- Someone or something with malicious intent has to be on your network or accessing your cloud environments.
- They have to be looking for your sensitive data.
- They have to find it.
- They have to move it.

This is true for every organization and leads us to the more important question: "How comfortable are you with your organization's ability to detect and respond when data is moving?"

There are three channels through which data loss occurs:

- Network Channel (e.g., email, web, File Transfer Protocol or FTP)
- Endpoint Channel (e.g., USB storage, printers, laptops, mobile phones, and tablets)
- Cloud Channels (e.g., Office 365, Box, Zoom, and Slack)

These are the channels where you can detect and respond to actual risks.

What About Data-at-Rest and Compliance?

Many regulations require you to scan your data stores for unprotected data-at-rest, so why wouldn't a DLP methodology and execution strategy start there? Actually, auditors are more concerned with the fact that you are complying over the span of the audit than whether you have complied in the past.

So scanning for data-at-rest is important to comply with HIPAA, GDPR, NIST, CIST, CSTAR, SOC-2 and other applicable government regulations and healthcare standards. However, compliance is not the primary objective and value of your DLP control. Therefore, plan on using DLP for data discovery and compliance, but in a way that is practical and sustainable for your organization.

The best place to start is to use DLP to automatically quarantine files that have not been accessed for at least six months. Assign permissions to your legal and compliance teams so they can make decisions based on data retention policies.

The Nine Steps to DLP Success

The following nine steps outline a practical, measurable process for implementing DLP controls. Whether your hospital is early in its DLP maturity or further down the path, these steps provide a results-driven blueprint for traditional DLP practitioners as well as those who want to augment their approach with risk-adaptive DLP.

Step 1:
Create an Information Risk Profile

Goal: Understand the scope of your data protection needs.
Actions: Create an initial information risk profile that includes:

→ The risk you want to mitigate.

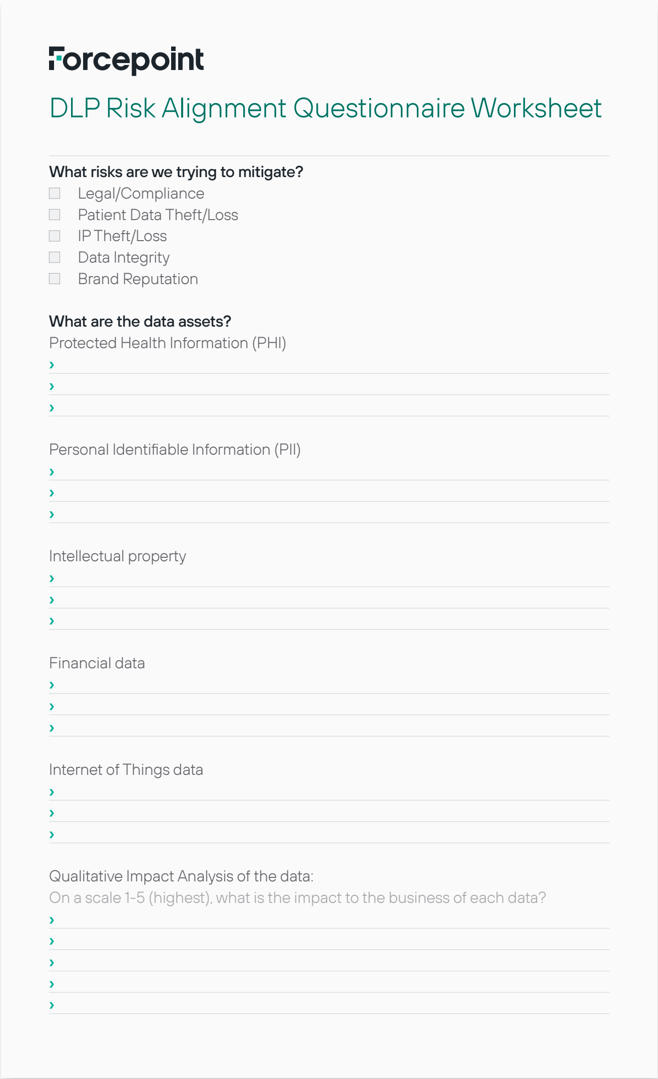
→ A statement of the potential consequences of inaction.

→ A list of data assets in scope, categorized by type (e.g., PII, PHI, IP, financial data).

→ Definitions of the network, endpoint, and cloud channels where information can be lost or stolen.

→ A qualitative impact analysis of the data, as indicated by the data owners.

→ A list of existing security controls currently used for data protection (e.g., encryption).



Forcepoint

DLP Risk Alignment Questionnaire Worksheet

What risks are we trying to mitigate?

□ Legal/Compliance
□ Patient Data Theft/Loss
□ IP Theft/Loss
□ Data Integrity
□ Brand Reputation

What are the data assets?

Protected Health Information (PHI)

›
›
›

Personal Identifiable Information (PII)

›
›
›

Intellectual property

›
›
›

Financial data

›
›
›

Internet of Things data

›
›
›

Qualitative Impact Analysis of the data:
On a scale 1-5 (highest), what is the impact to the business of each data?

›
›
›
›
›

Step 2:
Create an Impact Severity and Response Chart

Actions: Determine data-loss incident response times according to the degree of severity.

Overview: Ask your DLP implementation team to meet with data owners in your hospital to determine the level of impact if specific data is lost, stolen, or compromised. Use qualitative analysis to describe impact, such as a scale of 1–5. This helps to prioritize incident response efforts, and is used to determine the appropriate response time.

Risk-adaptive DLP Option: Keep in mind, a DLP solution that takes a risk-adaptive approach is designed to prioritize high-risk activity, autonomously enforce controls based on risk, and reduce the time it takes to investigate an incident. The result is lower risk of impact and more proactive control of critical data.

The steps outlined above still apply, but will be augmented with risk-adaptive DLP.

Regulations			**Step 1:** Discuss General Data Types **Step 2:** Relative Regulations (Wizard Avail) **Step 3:** "ID" — Registered or Described **Step 4:** Quantity or % for High Medium Low		Impact Rating Legend		
Breach Notification	HIPPA	FIPS 140-2			5, 4	3, 2	1
			Protected Health Information (PHI)	ID	High	Mod.	Low
🟩	▨	🟩	Name	R	1	-	-
🟩	▨	🟩	Social Security Number	D	>100	>25	>2
🟩	🟩	▨	Medical Test Results	D	>100	>50	>2
▨	▨	▨	Biometric Indicators				
▨	▨	▨	Medications/Prescriptions				
			Financial Information	ID	High	Mod.	Low
🟩	▨	🟩	Billing Amounts	D	>25	>5	>2
🟩	▨		Checking Account Information	D	>25	>5	>2
▨	▨	▨	Credit Card Numbers				
			Intellectual Property	ID	High	Mod.	Low
▨	▨	▨	Biomedical Research	R	>25%	>10%	10%<
▨	▨	▨	COVID-19 Treatment Processes	R	>25%	>10%	10%<
▨	▨	▨	User Names and Passwords	R	>25%	>10%	10%<
▨	▨	▨					

1. **Start by discussing the types of data to protect.**
2. **Align regulations with the data types identified.**
3. **Determine how you will identify the data.**
4. **Determine impact severity and incident response.**

Step 3:
Determine Incident Response Based on Severity and Channel

Goal: Define what happens in response to a data loss incident based on its severity and channel.

Actions: Your hospital has a limited number of channels through which information flows. These channels become the monitoring checkpoints that the DLP controls use to detect and respond to data loss. List all of the available communication channels on your hospital network, at the endpoint, and in the cloud (i.e., critical sanctioned and unsanctioned cloud applications) on a worksheet. Then apply a response (based on incident severity) using one of the response options available in the DLP controls for that channel.

You can also clarify any additional requirements that your hospital has for delivering the desired response, such as encryption or SSL inspection.

Quick Tip One option for mitigating the risk of data loss to Box or Google Drive is to automatically unshare files containing sensitive information that are transferred to cloud storage and shared externally.

Risk-adaptive DLP Option: A risk-adaptive DLP solution can provide hospitals with granular enforcement controls across channels, giving the flexibility to adjust response based on the risk level of the user (e.g., audit-only for low-risk users vs. block for high-risk users). This allows users to effectively perform their job duties, without compromising data.

1. **Choose data or data type**
2. **Confirm channels to monitor**
3. **Determine response based on severity**
4. **Note additional requirements for desired response**

Channels	Level 1 Low	Level 2* Low-Medium	Level 3 Medium	Level 4 Medium-High	Level 5 High	Notes
Web	Audit	Audit / Notify	Block / Notify	Block / Alert	Block	Proxy to Block
Secure Web	Audit	Audit / Notify	Block / Notify	Block / Alert	Block	SSL Inspection
Email	Encrypt	Drop Email Attachments	Quarantine	Quarantine	Block	Encryption
FTP	Audit	Audit / Notify	Block / Notify	Block / Alert	Block	Proxy to Block
Network Printer	Audit	Audit / Notify	Block / Notify	Block / Alert	Block	Install DLP Printer Agent
Cloud Applications	Audit	Audit / Notify	Quarantine with Note	Quarantine	Block	
Custom	Audit	Audit / Notify	Block / Notify	Block / Alert	Block	TBD

*Additional granularity available with risk-adapative DLP

Step 4:
Create an Incident Workflow Diagram

Goal: Ensure that procedures for identifying and responding to incidents are followed.

Actions: Create your workflow, referring to the diagram below as an example. Be sure to delineate a management process for each incident type. Your security incidents should represent various levels of severity and priority. For low-severity incidents, apply automation whenever possible; this typically includes notifying users and managers of risky behavior. It may also include staff coaching to facilitate self-remediation of risk.

Higher-impact incidents require intervention by an incident analyst, who will investigate and determine the type of threat (e.g., accidental, intentional, or malicious).

When the incident analyst completes an analysis, she will forward it and the incident details to the program manager—typically the head of security or compliance—who then determines what actions to take and which teams to include.

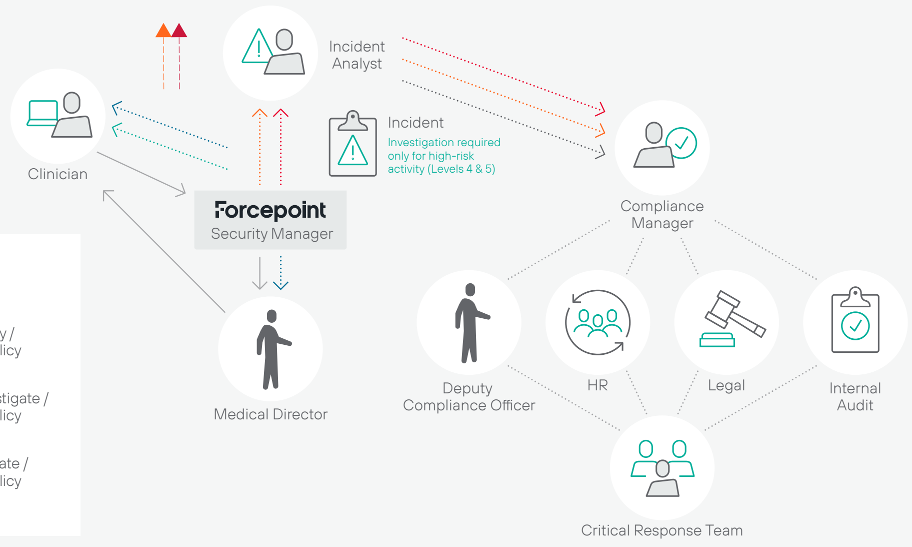
Risk-adaptive DLP Option: If you choose an adaptive solution, an incident analyst investigation is not required before action is taken. Incidents attributed to low-risk users may not pose a threat to the organization, and therefore should be permitted to avoid impacting productivity. Recognize, however, that these permitted actions include safeguards, such as requiring encryption when saving to USB or dropping attachments sent via email.

For higher-risk users and associated incidents, administrators can take a proactive approach by automatically blocking or restricting specific actions until the incident analyst can investigate.

Flow Based on Severity and Priority of Incident

With risk-adaptive DLP, policies are automatically enforced at every risk level

Low (Level 1)	Audit
Low-Med (Level 2)	Audit & Notify
Med (Level 3)	Restrict / Notify / Automated policy enforcement
Med-High (Level 4)	Restrict / Investigate / Automated policy enforcement*
High (Level 5)	Stop / Investigate / Automated policy enforcement*



Step 5:
Assign Roles and Responsibilities

Goal: Increase DLP program stability, scalability, and operational efficiency.

Actions: Typically, four distinct roles help preserve the integrity of the DLP controls and increase its operational efficiency.

→ Technical administrator

→ Incident analyst/manager

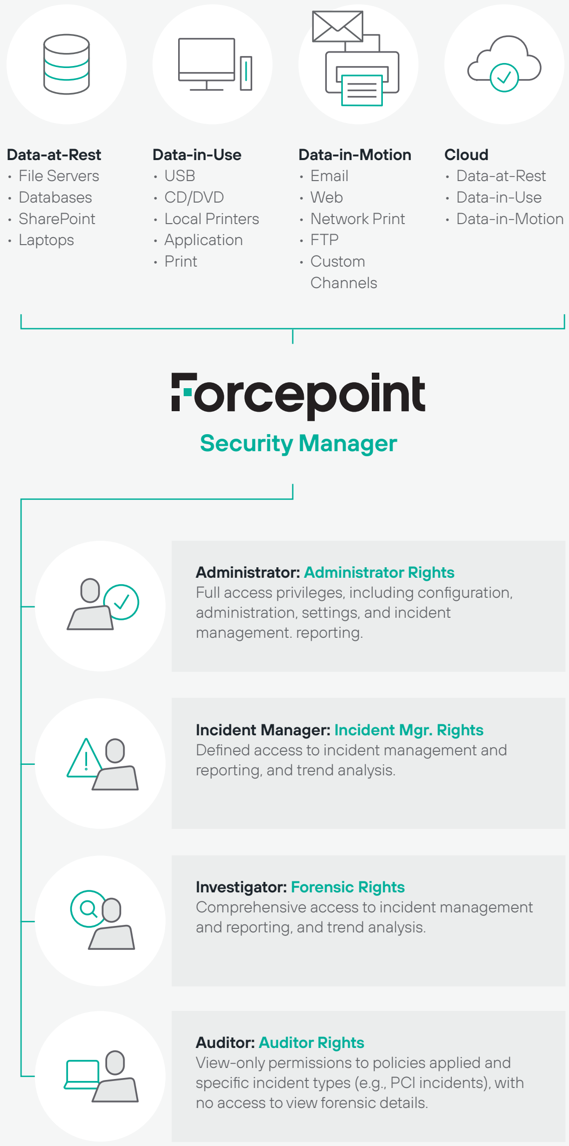
→ Forensics investigator

→ Auditor

Define each role according to its responsibilities and assign it to the appropriate stakeholder. At this stage, it's common for members of the DLP implementation team to act as incident managers. However, as DLP controls reach maturity and inspire a high level of confidence, these roles will be transitioned to the appropriate data owners.

Risk-adaptive DLP Option: If you choose an adaptive solution for your hospital, your policies will automatically adapt down to the individual user level, controlling data and access on premises, via endpoints, and in the cloud.

Assign roles and responsibilities



Data-at-Rest
- File Servers
- Databases
- SharePoint
- Laptops

Data-in-Use
- USB
- CD/DVD
- Local Printers
- Application
- Print

Data-in-Motion
- Email
- Web
- Network Print
- FTP
- Custom Channels

Cloud
- Data-at-Rest
- Data-in-Use
- Data-in-Motion

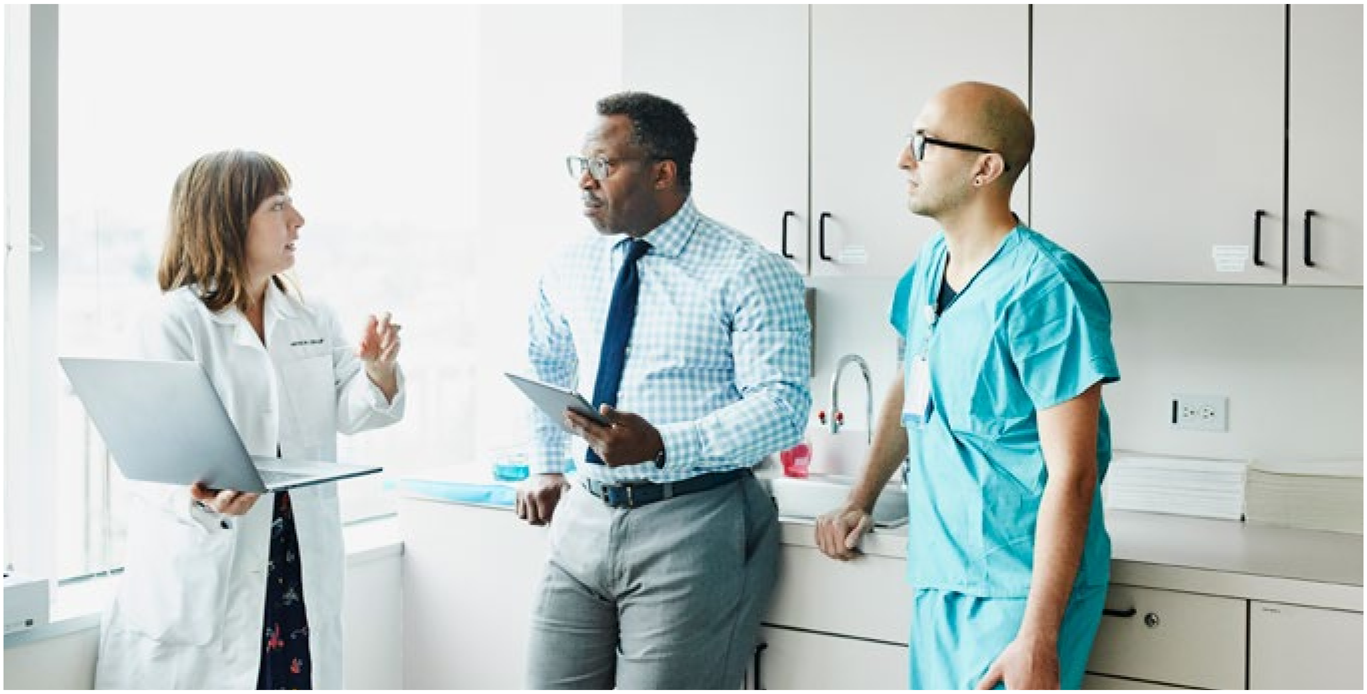
Forcepoint
Security Manager

Administrator: Administrator Rights
Full access privileges, including configuration, administration, settings, and incident management. reporting.

Incident Manager: Incident Mgr. Rights
Defined access to incident management and reporting, and trend analysis.

Investigator: Forensic Rights
Comprehensive access to incident management and reporting, and trend analysis.

Auditor: Auditor Rights
View-only permissions to policies applied and specific incident types (e.g., PCI incidents), with no access to view forensic details.



Step 6:
Establish the Technical Framework

Goal: Implement network DLP to measure and begin to reduce risk.

Actions: Step 6 has two phases. During phase one, you create a baseline to help your hospital recognize normal user behavior and prevent high-impact data breaches. At this stage, the role of the DLP control is primarily to monitor, blocking only high-severity incidents (e.g., data being uploaded to known malicious destinations or a mass upload of unprotected records).

As you gain more insight into data movement and usage within your hospital, you can adjust the controls to apply enforcement for higher-risk users.

After the initial monitoring phase, during which you deploy a network DLP control, conduct an analysis of monitoring data. This should include recommendations for risk mitigation activities that can reduce the RO (rate of occurrence) of data at risk. Then, capture the results and report them to the executive team.

Risk-adaptive DLP Option: If you choose to implement risk-adaptive DLP, you can run an analysis of incidents in audit-only mode versus graduated enforcement mode. This contrasting data will highlight the reduced number of incidents requiring investigation without compromising your data. Your results will better represent true positives. They can also demonstrate the benefits of automation, including less hands-on incident monitoring and management and fewer security interruptions for your staff as they go about their daily work.

✓ Step 9 covers ROI and the tracking of risk reduction in more depth.

1. **Install and configure**
2. **Monitor network**
3. **Analyze results**
4. **Executive update 1**
5. **Risk mitigation activities** (e.g., activate block policies)
6. **Analyze results**
7. **Executive update 2**

Step 7:
Expand DLP Control Coverage

Actions: Implement DLP to endpoints and sanctioned cloud applications to measure and begin to reduce risk.

Overview: Now you're ready to address data-in-use and data-at-rest. During this step, you deploy DLP to endpoints and cloud applications (sanctioned and unsanctioned), monitor and analyze your data, update the executive team, and perform risk-mitigation activities, much like you did in Step 6. The primary difference is that now you choose to respond to incidents based on the different channels and available options for data-in-use, which occur at the endpoint and in cloud applications. (You determined the incident severity and response according to channel in Step 3.)

For data-at-rest, identify and prioritize targets to scan and move any stale data to a quarantine, where your legal and compliance teams can proceed according to your organization's data retention policies. Regarding compliance, it's about cooperation—so cooperate, but at a speed that is reasonable for your hospital. Remember, nobody gets a prize for coming in first.

In case you need to perform a discovery task sooner rather than later, know that you can temporarily (or permanently) increase the speed at which discovery is performed by using local discovery agents, or by setting up multiple network discovery devices.

1. **Deploy endpoints and cloud applications (sanctioned & unsanctioned) and monitor**
2. **Start discovery scans**
3. **Analyze results**
4. **Executive update 3**
5. **Risk mitigation activities**
6. **Analyze results**
7. **Executive update 4**

Risk-adaptive DLP Option: If your hospital pursues risk-adaptive DLP, you'll have a holistic view of data as it moves outside your hospital's network, across endpoints, and into the cloud. This gives you and your team contextual clues into user intent, helping inform your security responses. It also establishes a security perimeter at a human level, ensuring patient and medical data is protected no matter where it's shared or accessed. Another advantage of risk-adaptive DLP: It applies on-network policies to off-network devices, such as those used by remote staff.

Step 8:

Integrate DLP Controls Throughout your Hospital

Goal: Delegate incident management to key stakeholders from major business units.

Action: If you haven't yet directly involved the data owners and other key stakeholders with the DLP implementation, now is the time.

In particular, the role of incident manager is best suited for the data owners, because they are liable in the event of data loss. Putting incident management in their hands eliminates intermediaries and improves operational efficiency. In addition, it enables them to accurately assess their risk tolerance and properly understand how their data assets are used by others.

During this step, ask the DLP implementation team to host a kickoff meeting to introduce the DLP controls to others. Follow this with training to acclimate the new team members to the incident management application. Before turning over incident management responsibilities, designate a transitional period. During this time, plan to assist with incident response to get the new team members up to speed.

Risk-adaptive DLP Option: With a risk-adaptive DLP solution, your security team has the opportunity to learn about the context of your hospital's security incidents. For example, they can understand what happens when a clinician emails PHI to a patient as opposed to that staff member saving the PHI to a USB stick. The latter may be a policy violation, or even a HIPAA violation if the USB stick is lost. Conversely, sharing electronic PHI via email may be permissible for some staff roles, but they must do it securely, on HHA terms.

1. **Create and engage committee**
2. **Program update and roles**
3. **Training**
4. **Assisted incident response**
5. **Executive update 5**
6. **Incident response by committee**
7. **Executive update 6**

Step 9:
Track the Results of Risk Reduction

Goal: Show ROI by demonstrating a measurable reduction in risk.

Actions: Consider these tips while executing the risk-reduction tracking process introduced in Step 6.

1. Group related incidents together.
Common groups include severity, channel, data type, and regulation. If your hospital is large, adding sub-groups will help to further clarify the risk according to geographic locations or subsidiaries.

2. Maintain consistency between risk-reduction phases.
To preserve the integrity of your results, the monitoring and risk-reduction periods should be of equal length. In the beginning, we recommend two weeks to improve time-to-value and to simplify analysis. However, you are in the best position to determine what is most reasonable for your hospital.

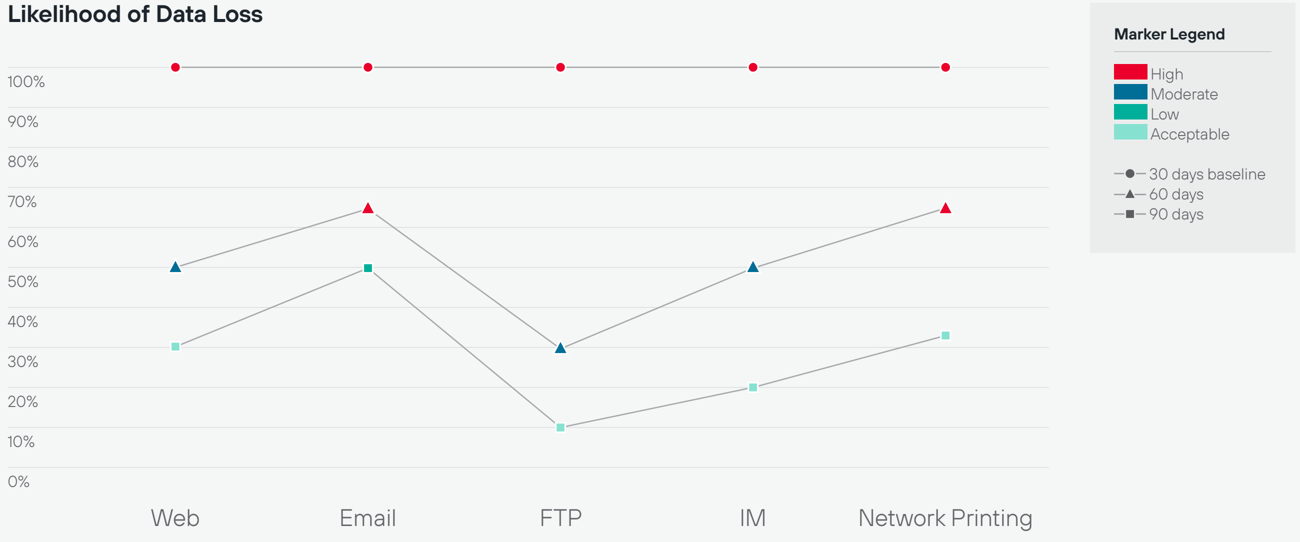
The graphic below is an example of incident grouping and risk reduction tracking. Note the consistent time period, high-risk incident focus, and incident grouping by specific channels.

Risk-adaptive DLP Option: If you have decided to take a risk-adaptive approach, you'll want to track the security incidents captured in audit-only mode (all incidents) versus incidents requiring investigation with graduated enforcement.

When updating your hospital's executive team on the DLP process and its results, be sure to show the number of incidents for each risk level from 1-5, contrasted against those actually requiring investigation (risk levels 4-5).

Finally, remember that less is more. Focus on the big picture as you explain your hospital's high-risk vectors and outline your recommended risk-mitigation activities highlighting the cost, benefits, and effort of each.

Likelihood of Data Loss



Number of Incidents over 90 Days

Incidents	Web	Email	FTP	IM	Network Printing
30 days baseline	200	150	50	10	45
60 days baseline	100	100	15	15	30
› 60-day risk reduction	50%	33%	70%	50%	33%
90 days baseline	60	76	5	2	15
› 90-day risk reduction	70%	49%	90%	80%	67%

Goals

✓ **60 days**
25% + reduction

✓ **90 days**
50% + reduction

Conclusion

You won't achieve a successful DLP implementation by switching on a new technical bell or whistle. DLP success can't be racked and stacked in your hospital's data center. Instead, it will depend on your ability to:

1. Understand how well a DLP solution's capabilities match your DLP goals and execution strategy. Your hospital benefits by discerning how different vendors approach DLP. Doing so allows you to determine the most promising vendors for your environment, and which DLP technologies to evaluate. Selecting a vendor with a risk-adaptive solution can create long-standing advantages for your hospital, including increased efficiency and productivity. And don't forget: applying one vendor's DLP vision (traditional or risk-adaptive) to another's technology can result in negative long-term implications.

2. Apply the risk formula for data loss. Once your security team understands and applies the risk formula for data loss, it can collaborate with data owners to identify and prioritize data assets. In addition, every risk-mitigation activity should be designed to lower the rate of occurrence (RO) of data loss. RO is the proper measurement for tracking risk reduction and showing the ROI for DLP controls. Remember, when comparing traditional DLP solutions to risk-adaptive DLP technology, avoid the trap of comparing false positives to real positives.

3. Allocate your security resources using the 80/20 rule as a guide. Start by understanding which data loss vectors pose the greatest risk of a high-impact data breach for your hospital. Use this knowledge to wisely allocate your resources and formulate effective data protection strategies.

4. Follow the nine steps to DLP success in this guide. Whether you take a traditional DLP approach or a risk-adaptive route, our nine-step process is a proven, practical formula for delivering actionable, measurable, and risk-adaptive results.

Questions about any of the steps in this guide? Wondering how Forcepoint can help you with your DLP strategy? Contact us!

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly-attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

[PRACTICAL-EXECS-GUIDE-TO-HOSPITAL-DLP-WHITEPAPER-EN] 6JAN2021