INFOLOCK

Educating Senior Leaders about Data Risk

WORKBOOK

Table of Contents

Section 1: Understanding and Engaging your Audience

1.1 Stakeholder Analysis

Objective

Identify and understand the key senior leaders and board members who play a crucial role in data risk management (DRM) decision-making.

Identify Stakeholders

List out the roles and names of all of your key stakeholders related to data risk management decision making. *Helpful Tip: Stakeholders may include Board Members, C-Level Executives, Department Heads, etc.*

Stakeholder Concerns & Perceptions

Interview each stakeholder one on one to better understand their current data risk concerns, perceptions, and priorities. Use the questions outlined below as a guide, but also consider brainstorming additional questions that would be unique to your industry and organization.

1. What are your primary concerns about organizational data risk?
2. How do you perceive the current state of data risk management in the organization?
3. What past incidents or discussions have influenced your current view of data risk management within the organization?
4. What type of update method do prefer when it comes to being informed about data risk concerns, priorities, projects, and outcomes? What level of detail are you hoping to see?
5. What type of frequency do you expect those updates?

Influence & Impact Matrix

Fill out the Influence & Impact Matrix on the next page to plot the key stakeholders based on their level of influence and impact on your organization's data risk management program. This exercise will you help you prioritize engagement efforts. *Helpful Tip: Check out the Matrix Definitions to see the description and examples of the types of stakeholders that best fit in each quadrant.*

High Influence, High Impact (Keep Satisfied)	**High Influence, Low Impact (Keep Informed)**
Low Influence, High Impact (Monitor)	**Low Influence, Low Impact (Minimal Effort)**

Matrix Definitions

01. High Influence, High Impact (Keep Satisfied)

Description: Stakeholders in this quadrant have a significant influence on the project or initiative and are highly impacted by its outcomes. They are key players and their support is crucial for the success of the initiative.

Examples: CEO, Board of Directors, Regulatory Authorities.

Strategy: Engage these stakeholders closely, ensure they are fully informed, and prioritize their concerns and feedback.

02. High Influence, Low Impact (Keep Informed)

Description: Stakeholders here have a significant influence on the initiative, but are less affected by its outcomes. They can sway decisions but might not be the primary beneficiaries or victims of those decisions.

Examples: Senior Management, IT Department Heads, Legal Team.

Strategy: Keep them well-informed about progress and decisions. Regular updates are key, but detailed involvement might not be necessary.

03. Low Influence, High Impact (Monitor)

Description: These stakeholders are highly affected by the initiative's outcomes but have limited power to influence it. Their needs and concerns are important from an ethical and operational perspective.

Examples: End-users, Junior IT staff, External Partners.

Strategy: Ensure their concerns are addressed, even if they don't have the power to drive decisions. Regular feedback loops can be beneficial.

04. Low Influence, Low Impact (Minimal Effect)

Description: Stakeholders in this quadrant have limited influence over the initiative and are minimally affected by its outcomes.

Examples: External vendors (not directly related), departments not interacting with IT systems.

Strategy: Keep them informed through general communications but focus less effort on detailed engagement.

Section 2: Translating Security Jargon into Business Terms

2.1 Glossary Creation

Objective

Develop a comprehensive glossary that translates technical terms and concepts central to data risk management into business-centric definitions or analogies.

List of Common Industry Terms

Create a list of technical terms frequently used when discussing data risk management, such as "data security," "data protection," "data privacy," etc. Then, beside each technical term, write a simplified definition or analogy that can be easily understood by non-technical stakeholders. For example, "data risk management" is defined as “a strategic business discipline for analyzing and mitigating threats to an organization's data assets. Identifies, assesses, and controls both down-side and upside risks to data.”

Helpful Tip: Check out Infolock’s Industry Glossary to pull relevant terms and definitions for your organization.

2.2 Quantifying the Real World Impact

Objective

Gather credible data that demonstrates the real-world impact of data breaches and security incidents.

Guidelines on Sourcing Credible Statistics and Case Studies

1. Diversify Your Sources: Use a mix of industry reports, academic research, and news articles to gather data. This ensures a comprehensive view of the topic.

2. Prioritize Recent Data: While historical context is essential, prioritize data from the last 1-3 years to ensure relevance.

3. Verify Authenticity: Ensure that the data is sourced from reputable organizations or experts in the field. Cross-reference facts when possible.

4. Document Your Sources: Always note down where you sourced particular data for easy reference and to maintain transparency.

Use this space below for collecting your research notes:

1. Industry Report Findings:

2. Academic Research Insights:

3. Relevant News Articles:

2.3 Crafting the Impact Slide

Objective

Create a compelling slide that succinctly demonstrates the financial and operational impact of data-related incidents.

Tips on Presenting Data Effectively

1. Keep It Simple: Avoid clutter. Each slide should convey one main idea or point.

2. Use Visuals: Graphs, charts, and infographics can often communicate data more effectively than text alone.

3. Highlight Key Figures: If there's a particularly striking statistic, make it stand out using **bold**, larger font, or a different color.

4. Maintain Consistency: Use consistent fonts, colors, and styles to ensure that each slide looks professional and is easy to read.

A template for a Data Risk Management Impact Slide could contain:

1. Slide Title: The Tangible Impact of Data Breaches

2. Key Statistic: XX% of companies faced operational disruptions due to data breaches in the past year.

3. Supporting Data/Graph: [Space for a brief description to accompany a graph/chart]

4. Case Study Highlight: Company Y faced a loss of $XX million due to a data breach in Q1 20XX.

2.4 Highlighting Business Accomplishments over Security Concerns

Objective

Underscore the positive impact of the data risk management program on the organization by shifting the narrative from mere security concerns to tangible business outcomes.

List out Data Risk Management Program Accomplishments

Compile a list of significant milestones achieved by the data risk management program over a fixed amount of time (e.g., the last 12 months, the last quarter, etc).

Example: "Successfully conducted Business Unit Data Risk Assessments across 45% of the enterprise."

Anecdotal Evidence & Case Studies

Document specific incidents where the DRM program played a crucial role, and detail the resolutions.

Example: "In March 2022, our system detected a large number of customer files being copied to an external site, potentially in breach of our customer terms of agreement. Due to our DRM protocols, the incident was identified and mitigated within hours, preventing any data loss and potential harm to our customer relationships."

Quantifying Value

Translate DRM actions into tangible business value, showcasing the financial and operational benefits.

Example: "Our proactive measures, including regular system audits and employee training, prevented potential losses of $5M in 2022 by thwarting data breaches."

2.5 Feedback Mechanism

Objective

Establish a continuous loop of feedback to ensure the DRM program remains effective and evolves with the changing threat landscape. Celebrate successes and learn from challenges.

Regular Check-ins

Create a realistic calendar for the next 12 months that maps out regular feedback sessions with the team to discuss the effectiveness of the DRM program.

Example: Weekly team debriefs where members discuss challenges faced, share success stories, and brainstorm improvements.

Feedback Channels

Set up dedicated channels for team members to provide immediate feedback or report concerns.

Example: Create a dedicated Slack channel named "DRM Feedback" or an email alias like "drmfeedback@company.com" where team members can share insights, concerns, or suggestions.

Recognition & Rewards

Recognize and celebrate the efforts of team members who go above and beyond in ensuring the success of the DRM program.

Example: Introduce a "DRM Champion" award every quarter, recognizing an individual or team that has made significant contributions to the DRM program. This could include cash rewards, certificates, or public recognition in company meetings.

Section 3: Show a Plan

3.1 Enabling Business Transformation

Objective

Strategize for upcoming business transformations, ensuring they're efficient and secure.

Outline your Data Risk Management Maturation Plan

In today's rapidly evolving digital landscape, it's not enough to just maintain the status quo. As a data risk management executive, you're tasked with not only safeguarding the present but also charting a secure course for the future. Outline your plan for improving upon current data risk management efforts. Some possible forward-thinking initiatives could be:

1. **Plans for Cloud Transformation:**
    a. Detail the roadmap for migrating to the cloud or enhancing cloud security.
    b. Discuss potential challenges and strategies to mitigate them.
    c. Ensure security during digital transitions.
    d. Share plans for securing other digital transformations, such as IoT integration or AI

2. **Vendor Consolidation: Streamline vendor relationships to achieve efficiency and cost savings.**
    a. Impact on cost savings and effficiency:
        i. Discuss the projected financial benefits of this consolidation.
        ii. Highlight any anticipated improvements in operational efficiency.

3.2 Pitching the Vision

Objective

Illuminate the new business avenues made possible by proactive security measures and cost saving measures.

Where do I start?

Outline the new opportunities that enhancing the organization's data risk management program unlocks. Show leadership how wise the team has been with the resources entrusted to them thus far. Some examples could include:

1. New Markets or Sectors

Example: "Our enhanced security protocols now allow us to enter the healthcare sector, adhering to its stringent data protection requirements."

2. Business Collaborations

Example: "Our robust security posture has facilitated a partnership with Company X, known for its strict vendor security criteria."

3. Cost Efficiency and ROI

Example: "Our Data Inventory initiative enabled us to reduce our data footprint by 50%."

4. Investment Justification

Example: "Transitioning to a managed DLP service provider will enable our team to focus on mission-critical activities, ensure seamless incident response, and mature our DLP program under the guidance of subject matter experts."

Section 4: Implement Effective Reporting

4.1 Key Performance Indicators (KPIs)

Objective

Establish and track metrics that demonstrate the efficacy of the DRM program.

Where do I start?

Outline the following:

1. List of Potential KPIs

a. Collaborate with the analytics team. *Example: "Average Response Time to Data-related Incidents."*

2. Alignment with Business Objectives

a. Match KPIs with company goals. *Example: If a company goal is to ensure compliance with GDPR, a KPI might be "Percentage of Data Mapped: Track the percentage of personal data within your organization that has been identified, categorized, and documented in your data inventory. "*

3. Set Targets

a. Set achievable, yet challenging targets. *Example: "15% of Data Mapped by Q3."*

4.2 Visual Representation

Objective

Transform data into engaging visual representations.

Where do I start?

Here are the 3 main steps to follow when developing compelling KPI visuals:

1. Choose the right visuals: Collaborate with the organization's design team, a freelance graphic designer that can easily be contracted (such as from platforms like Fiverr), or leverage easy to use design template websites like Canva. *Example: Use charts to show the distribution of different types of data incidents and related trends.*

3. Create Dashboards: Use tools like Tableau or PowerBI and/or work with your internal data analytics team to develop the dashboard. Templates or freelance developers can also be found online on platforms like Fiverr. ***Example: A live dashboard showing real-time threat levels, incidents, and resolutions.***

4. Tell a Story with the Data: Create a narrative around the data. ***Example: A year-end review showing the company's DRM journey, challenges, and victories.***

Section 5: Ask for Support

5.1 Who are your internal champions and cheerleaders?

Objective

Identify senior stakeholders who will evangelize data risk management efforts within your organization.

Where do I start?

Revisit the Influence & Impact Matrix in Section 1. Reflect on the stakeholders outlined in that matrix and try to identify 1-2 key influencers within the organization who carry both authority and respect from their peers.

Identify ways they can organically champion data risk management efforts internally, like sending out an organization-wide email when a new training becomes required that optimistically encourages employees to complete the training.

Section 6: Conducting Tabletop Exercises

6.1 Introduction to Tabletop Exercises

Objective

Learn all about tabletop exercises - the concept and their advantages.

What are Tabletop Exercises?

Tabletop exercises are simulated scenarios that test an organization's response to a hypothetical situation. They are discussions based on a narrative, allowing participants to understand and practice their roles in a safe environment. The exercises identify gaps in the response plan, while also enhancing communication and collaboration among teams.

What do I need to do in preparation for the tabletop exercise?

Step 1: Outline your organization's current data risk management measures and gaps by listing off all existing data security measures and pinpointing any known gaps.

1. Possible Existing Measures:

a. Regular data backups

b. Employee training on phishing and malware

c. Advanced threat detection systems

2. Possible Existing Gaps:

a. Outdated security infrastructure

b. Lack of a dedicated incident response team

3. After outlining your DRM measures and gaps, reflect on the following:

a. What resources or support do you believe is necessary to address these gaps?

b. Are there other potential vulnerabilities you're aware of?

Step 2: Outline your Incident Response Plan. An Incident Response Plan (IRP) is a well-structured approach that details the processes to follow when a cybersecurity and/or data breach incident occurs. Having a plan in place prior to a security event ensures a quick and effective response to threats. A well-organized plan also minimizes damage and reduces recovery time and costs.
Helpful Tip: If your company already has a well-defined IRP, then have participants re-read the plan prior to the tabletop exercise as pre-work for the meeting. Have hard copies of the plan printed out and available for everyone on the day of the exercise

Step 3: Outline all pertinent roles and responsibilities so that the whole team understands the role each senior leader plays during a data-related incident. Ensure everyone participating in the exercise knows their general role and responsibility prior to the meeting.

Common Role Breakdown:

a. CEO: Communication with stakeholders and media.
b. CFO: Financial implications and potential settlements.
c. CISO: Overseeing the technical response and mitigation strategies.

6.2 Conducting the Exercise

Objective:

Facilitate a simulated data breach scenario amongst your organization's senior leadership.

Scenario

The organization has just been hit by a ransomware attack. Ransomware is a type of malicious software that encrypts an organization's data, rendering it inaccessible. The attackers have demanded a ransom in exchange for the decryption key. How are we going to respond?

Helpful Tip: Record the exercise so you can watch playbacks – similar to a Quarterback watching game tapes to see why he threw an interception.

Debrief and Reflection

Once the breach has been contained and all regulatory notification and brand reputation communication efforts have been executed, reflect on the exercise and gather insights.

Questions for Reflection

Q1. What went well during the exercise?

Q2. Where were the challenges?

Q3. What improvements can be made to our response plan?

Q4. Are there areas where additional training might be beneficial? Crisis communication? Understanding cybersecurity basics? Legal implications of data breaches?

About Infolock

Founded in 2005, Infolock is the go-to data risk management advisory, consulting, and managed services firm for security conscious organizations. With a programmatic approach, Infolock expertly manages the complex data risks of its clients, enabling organizations to achieve their strategic business objectives. Named among the "Fastest Growing Companies" on Inc. Magazine's "Inc. 5000" list, Infolock developed DataRAMP™, a data risk management framework which empowers organizations to understand and manage data risk in the same manner as other organizational risks, such as financial, competitive, and regulatory risk. Headquartered in Arlington, VA, Infolock serves customers in the financial services, healthcare, government, educational and other highly-regulated industries around the world. **Learn more at infolock.com**.

2900 South Quincy Street Suite 330
Arlington, Virginia 22206

Web: www.infolock.com
Email: info@infolock.com

Local: (202) 600-7270
Toll free: (877) 610-5625